Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet

Koops, E.J.; Bekkers, R.N.A.; Bongers, F.J.; Fijnvandraat, M.

Publication date:
2005

UNIVERSITEIT VAN TILBURG

Aftapbaarheid van telecommunicatie

Een evaluatie van hoofdstuk 13 Telecommunicatiewet

Bert-Jaap Koops
Rudi Bekkers
Frank Bongers
Marieke Fijnvandraat

TILT – Centrum voor Recht, Technologie en Samenleving
Dialogic *Innovatie & Interactie*

Tilburg, november 2005

TILT - Centrum voor Recht, Technologie en Samenleving
Postbus 90153 • 5000 LE Tilburg • Bezoekadres > Warandelaan 2 • Tilburg • Telefoon 013 466 81 99 • www.uvt.nl/tilt/

Inhoudsopgave

Afkortingen

ADSL	Asynchronous Digital Subscriber Line
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene Maatregel van Bestuur
AT	Agentschap Telecom
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CALEA	Communications Assistance for Law Enforcement Act
CBP	College Bescherming Persoonsgegevens
CIOT	Centraal informatiepunt onderzoek telecommunicatie
DGTP	Directoraat-Generaal Telecom en Post
ETSI	European Telecommunications Standards Institute
EZ	Ministerie van Economische Zaken
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications / Groupe Spéciale Mobile
ICT	informatie- en communicatietechnologie
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv6	Internet Protocol versie 6
ISDN	Integrated Services Digital Network
ISP	Internetaanbieder (Internet Service Provider)
ITU	International Telecommunication Union
ivd	inlichtingen- en veiligheidsdienst
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAW	naam, adres en woonplaats
NBIP	Nationale Beheerorganisatie Internet Providers
NLIP	branchevereniging van Nederlandse Internet Providers
OPTA	Onafhankelijke Post- en TelecommunicatieAutoriteit
p2p	peer-to-peer
PDA	Persoonlijke Digitale Assistent
SIP	Session Initiation Protocol
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TFTS	Terrestrial Flight Telephone [Telecommunications] System
TIIT	Transport of Intercepted IP Traffic
TW	Telecommunicatiewet
UMTS	Universal Mobile Telecommunications System
VMNO	Virtual Mobile Network Operator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
Wtv	Wet op de telecommunicatievoorzieningen

Managementsamenvatting

Aftappen is van groot belang voor de opsporing en de nationale veiligheid. De waarde van dit middel voor justitie en veiligheidsdiensten is onomstreden en staat niet ter discussie. Om te kunnen aftappen, moet telecommunicatie echter wel aftapbaar zijn. Dit onderzoek gaat over de vraag hoe aftapbaarheid het beste gewaarborgd kan worden.
Deze studie, geschreven in opdracht van het Ministerie van Economische Zaken, evalueert het aftapbaarheidsbeleid zoals dat is vastgelegd in hoofdstuk 13 Telecommunicatiewet (TW). 'Aftapbaarheid' duidt op het veiligstellen van de mogelijkheid tot onderzoek van telecommunicatie (aftappen, en vorderen van gebruikers- en verkeersgegevens). Hoofdstuk 13 TW legt verplichtingen op aan de aanbieders van openbare telecommunicatie om deze aftapbaarheid te waarborgen.
Het aftapbaarheidsbeleid dateert uit de periode 1996-1998, met het *Beleidsvoornemen bevoegd aftappen telecommunicatie* en de vertaling daarvan in de Telecommunicatiewet in 1998. De telecommunicatie ontwikkelt zich echter voortdurend, zowel in de markt als in de techniek, waardoor de aftapbaarheid van telecommunicatie onder druk staat. Het doel van deze studie is te verkennen of het aftapbaarheidsbeleid in het verleden adequaat is vertaald in wet- en regelgeving, en of beleid en wetgeving adequaat zijn voor de toekomst in het licht van ontwikkelingen in de telecommunicatie.
Dit evaluatieonderzoek richt zich grotendeels op de drie belangrijkste pijlers van beleid en wetgeving, te weten de algemene verplichting dat openbare telecommunicatie aftapbaar moet zijn, de meewerkplichten voor telecomaanbieders, en de kostenverdeling. Het onderzoek, dat vanwege beperkte middelen is uitgevoerd als een kwalitatieve, en geen kwantitatieve, evaluatie, is uitgevoerd door middel van interviews met behoeftestellers (justitie en inlichtingen- en veiligheidsdiensten), telecomaanbieders, toezichthouders en andere deskundigen, aangevuld met literatuuronderzoek. De bevindingen van het onderzoek bevatten voor een belangrijk deel de meningen van behoeftestellers en aanbieders; de conclusies en aanbevelingen komen voor rekening van de onderzoekers.

Onderzoeksvraag 1. Zijn de beleidsuitgangspunten uit 1996 voor aftapbaarheid adequaat vertaald in wet- en regelgeving?
De beleidsuitgangspunten uit 1996 zijn elk adequaat vertaald in wet- en regelgeving. Het beleid als geheel is ook adequaat geïmplementeerd in wet- en regelgeving, aangezien de aftapbaarheid van openbare telecommunicatie grotendeels gerealiseerd is en aldus het doel van het beleid – het behoud van het middel aftappen – grotendeels bereikt wordt. De aftapbaarheid is echter niet volledig gerealiseerd – en behoeftestellers noemen het niet-aftapbare deel ernstig – door enerzijds te laat op gang gekomen handhaving en een niet-optimale verstandhouding tussen behoeftestellers en aanbieders, en anderzijds de complexiteit en diversificatie in de telecommunicatiesector.

Onderzoeksvraag 2: Zijn de beleidsuitgangspunten en de huidige wet- en regelgeving voor aftapbaarheid voldoende toegesneden op huidige en toekomstige ontwikkelingen in telecommunicatie?
Op basis van de vraaggesprekken en de literatuurstudie over ontwikkelingen in telecommunicatie zijn vijf probleemvelden gesignaleerd. Deze liggen op het vlak van de technische aftapbaarheid in relatie tot de kostenproblematiek; de meewerkplichten staan niet onder druk door deze ontwikkelingen en kunnen dus worden gehandhaafd. De probleemvelden kunnen grofweg als volgt worden samengevat:

1. de handhaving staat nog in de kinderschoenen, er is onvoldoende spontane naleving, en de onderlinge verstandhouding tussen behoeftestellers en aanbieders is niet optimaal;
2. aan het wettelijke vereiste dat aftapbaarheid al bij introductie van een netwerk of dienst is bewerkstelligd, wordt niet voldaan, en dit is ook een onrealistische eis. Nieuwe vormen van telecommunicatie(diensten) vragen wellicht om andere technische uitvoeringsregelgeving. Dit vraagt om discussie en/of onderzoek naar een adequate oplossing.
3. de huidige wetgeving is sterk geënt op de situatie uit het verleden, waarin het vooral om telefonie ging en er slechts een klein aantal, relatief grote aanbieders op de markt actief waren. De huidige situatie, zijnde een divers en complex telecomlandschap met veel – ook

kleinere – aanbieders, vraagt om specifiekere, op de verschillende situaties afgestemde regels waarbij met name een onderscheid tussen telefonie en internet op zijn plaats is. Het streven naar een volledig techniekonafhankelijke wetgeving is gezien de ontwikkelingen niet langer mogelijk;
4. openbaarheid van telecommunicatie is geen geschikt aanknopingspunt voor wettelijke aftapbaarheidsplichten omdat het als zodanig niet relevant is voor de aftapbaarheidsbehoefte, en ook omdat de investeringskosten bij kleine openbare netwerken en diensten onevenredig hoog kunnen zijn; de aftapbepalingen passen niet goed in het kader van de primair marktordenende Telecommunicatiewet, en de positie van EZ heeft in de praktijk weinig meerwaarde als bemiddelende factor tussen aanbieders en behoeftestellers;
5. door diverse technische en marktontwikkelingen nemen effectiviteit en efficiëntie van de aftapbaarheidswetgeving af; dit komt grofweg doordat enerzijds verkeersstromen minder goed bij bepaalbare of aanspreekbare aanbieders zijn op te vragen of überhaupt niet meer bij dienstaanbieders langskomen, en anderzijds doordat het tappen op netwerkniveau theoretisch wel mogelijk is maar minder individualiseerbare of interpreteerbare signalen oplevert.

Het bovenstaande betekent overigens niet dat we de medewerkingsverplichting voor aanbieders die wel één of meer componenten van de intergrale telecommunicatiedienst leveren als zodanig ter discussie stellen.

Op basis van deze probleemvelden is de conclusie gerechtvaardigd dat bij voortzetting van de huidige beleidsuitgangspunten en de huidige wetgeving in de toekomst steeds meer knelpunten zullen ontstaan, waardoor steeds minder tegen aanvaardbare kosten een voor de behoeftestellers adequaat niveau van aftapbaarheid kan worden gegarandeerd. Daarom zullen keuzes gemaakt moeten worden in beleid en wetgeving, wil men het instrument aftappen ten minste in redelijke mate kunnen behouden.

Onderzoeksvraag 3: Indien de beleidsuitgangspunten of de huidige wet- en regelgeving onvoldoende zijn toegesneden op de gesignaleerde telecommunicatieontwikkelingen, welke oplossingen zijn dan denkbaar die beter invulling zouden kunnen geven aan de behoeften tot aftappen van de behoeftestellers, met inachtneming van de belangen van aanbieders?
In onderstaande tabel geven wij een indicatie van mogelijke oplossingen voor de gesignaleerde problemen. Wij formuleren de oplossingen in de vorm van aanbevelingen.

probleemveld	aanbevelingen
1: handhaving, spontane naleving en de onderlinge verstandhouding tussen behoeftestellers en aanbieders	• De handhaving door Agentschap Telecom moet worden voortgezet en uitgebouwd, zeker waar achterstanden zijn ontstaan ten aanzien van het aftapbaar maken van systemen; de overheid moet zo nodig extra investeren in handhaving; • de verstandhouding tussen aanbieders en behoeftestellers moet worden verbeterd door inspanningen aan beide kanten om beter te communiceren, door investeringen in kennis en kunde op de werkvloer (niet alleen maar wel met name bij de behoeftestellers), en door meer openheid (bij aanbieders over technische ontwikkelingen, en bij de overheid over gebruik en nut van het instrument aftappen).
2: aftapbaarheid bij introductie	• De eis dat aftapbaarheid *op het moment van introductie* is verzekerd, moet niet strikt worden gehandhaafd; • bij ingrijpende vernieuwingen in de telecommunicatie moet het instrument ontheffing (art. 13.8 TW) worden gebruikt om een overgangssituatie te scheppen waarin gezamenlijk, bij voorkeur in Europees verband, aan aftapbaarheid kan worden gewerkt; zo nodig moet daartoe (de interpretatie van) de clausule ‘in bijzondere gevallen’ van art. 13.8 worden aangepast;

	• bij ontheffingverlening kan worden gestipuleerd dat de aanbieder moet dulden dat de behoeftestellers zelf op zijn netwerk of dienst komen tappen; • Nederland zou zich kunnen inspannen voor de ontwikkeling van Europese en internationale normen en voor afstemming tussen EU-lidstaten waar het de overdrachtstechnieken betreft.
3: te simpele transponering van beleid, de wetgeving is te techniekonafhankelijk	• De wetgever moet alle beleidsuitgangspunten en individuele wettelijke bepalingen, waaronder de kostenverdeling, hetzij herbevestigen hetzij herzien, onderbouwd met argumenten voor de huidige situatie, en niet langer redeneren vanuit de historische situatie; • de wetgever moet bij aftapgerelateerde wetgeving, zoals het CIOT en bij een eventuele algemene bewaarplicht voor verkeersgegevens, onderscheid maken tussen telefonie en Internet omdat daar fundamenteel verschillende situaties bestaan.
4: openbaarheid, het aanknopingspunt van wettelijke plichten, relatief hoge kosten voor kleine netwerken of diensten, en de positie van EZ	• De wetgever moet overwegen het criterium van openbaarheid als aanknopingspunt voor de aftapbaarheidsplichten te vervangen door een ander criterium; • het verdient sterke overweging om, in plaats van het huidige regime, de aftapbaarheidsplichten slechts op te leggen aan partijen die telecommunicatie faciliteren met een bepaalde minimumomvang; onder de drempelwaarde hoeft men niet op eigen kosten aftapbaarheid in te bouwen, maar moet men wel dulden dat de behoeftestellers zelf langskomen om eigen tapapparatuur aan te sluiten; • het verdient overweging de aftapbaarheidsplichten uit de Telecommunicatiewet te halen en onder te brengen in een zelfstandige wet onder verantwoordelijkheid van Justitie, BZK en Defensie.
5: afnemende effectiviteit en efficiëntie door diverse technische en marktontwikkelingen	• De overheid dient de komende jaren na te gaan of de door ons verwachte tendens van afname in betekenisvol tappen zich inderdaad voordoet; • de overheid dient te onderzoeken welke mogelijkheden er zijn om deze eventuele afname tegen te gaan, en hoeveel die mogelijkheden kosten, zowel qua financiële investeringen bij aanbieders en overheid, als qua gevolgen voor innovatie, mededinging en privacy; • de overheid dient in de beleidsvorming rond opsporingsmethoden rekening te houden met de mogelijkheid van een langetermijnscenario waarin het vermogen om betekenisvol af te tappen significant afneemt, tenzij tegen buitensporige kosten; • om een te grote terugval te voorkomen in de mate van betekenisvolle aftapbaarheid zal het nodig zijn substantieel te investeren in kennis, menskracht en apparatuur bij de behoeftestellers.

1. Inleiding

1.1. Aanleiding, doel en vraagstelling

Aftappen is van groot belang voor de opsporing en de nationale veiligheid. De waarde van dit middel voor justitie en veiligheidsdiensten is onomstreden en staat niet ter discussie. Om te kunnen aftappen, moet telecommunicatie echter wel aftapbaar zijn. Dit onderzoek gaat over de vraag hoe aftapbaarheid het beste gewaarborgd kan worden.
Deze studie is geschreven in opdracht van het Ministerie van Economische Zaken. De opdracht betrof het evalueren van het aftapbaarheidsbeleid zoals dat is vastgelegd in hoofdstuk 13 Telecommunicatiewet. Aftapbaarheid wil zeggen dat telecommunicatie technisch onderschept kan worden op het netwerk of bij de dienst waarover deze wordt vervoerd (technische aftapbaarheid) en dat aanbieders van telecommunicatie meewerken met een last tot onderscheppen van telecommunicatie (organisatorische aftapbaarheid). Het betekent ook dat gegevens over telecommunicatie (verkeersgegevens) en gegevens over telecomgebruikers (gebruikersgegevens) verstrekt kunnen worden. 'Aftapbaarheid' duidt dus op het veiligstellen van de mogelijkheid tot onderzoek van telecommunicatie. Om stilistische redenen en vanwege de ingeburgerdheid van de term 'aftapbaarheid' zal in dit rapport vaak 'tappen', 'aftappen' 'taplast' en dergelijke worden gebruikt waar 'onderzoek van telecommunicatie' bedoeld wordt, dat wil zeggen dat het betreft het onderscheppen van telecommunicatie en/of het vorderen van verkeers- en/of gebruikersgegevens.
Hoofdstuk 13 van de Telecommunicatiewet (TW) legt verplichtingen op aan de aanbieders van openbare telecommunicatie om deze aftapbaarheid te waarborgen. Het betreft hier een prototype van het spanningsveld tussen publieke en private belangen: private partijen worden verplichtingen – en in dit geval ook kosten – opgelegd die het publieke belang beogen te waarborgen. Het belang van de private partijen, de aanbieders van telecommunicatie, om naar eigen inzicht en marktconform netwerken en diensten te ontwikkelen en beheren strijdt hier met het publieke belang van die overheidsdiensten, de behoeftestellers,[1] die behoefte hebben aan aftappen van telecommunicatie en daarmee aan aftapbaarheid. De reikwijdte van de verplichtingen, en met name ook van de kosten die deze verplichtingen met zich meebrengen, is daarom een gevoelig en politiek beladen onderwerp.

De *aanleiding* voor de evaluatie is het feit dat het aftapbaarheidsbeleid dateert uit de periode 1996-1998, met het Beleidsvoornemen bevoegd aftappen telecommunicatie[2] en de vertaling daarvan in de Telecommunicatiewet in 1998, en dat zich sindsdien forse ontwikkelingen hebben voorgedaan in de telecommunicatie, zowel in de markt als in de techniek. Bovendien gaan deze ontwikkelingen steeds voort, bijvoorbeeld met glasvezel- en Internettelefonie, en lijkt er vooralsnog geen einde te komen aan nieuwe technieken die de aftapbaarheid van telecommunicatie onder druk zetten. Deze ontwikkelingen roepen de vraag op of de uitgangspunten uit 1996 en de vertaling daarvan in wetgeving sinds 1998 nog steeds bruikbaar zijn voor de huidige en de toekomstige situatie.

Het *doel* van deze studie is te verkennen of het aftapbaarheidsbeleid in het verleden adequaat is vertaald in wet- en regelgeving, en of dit beleid en deze wetgeving voor de toekomst adequaat zijn in het licht van ontwikkelingen in de telecommunicatietechniek en -markt. Deze doelstelling leidt tot een drieledige *vraagstelling* die centraal staat in dit onderzoek:

1. Zijn de beleidsuitgangspunten uit 1996 voor aftapbaarheid adequaat vertaald in wet- en regelgeving[3]?
2. Zijn de beleidsuitgangspunten en de huidige wet- en regelgeving voor aftapbaarheid voldoende toegesneden op huidige en toekomstige ontwikkelingen in telecommunicatie? Dat wil zeggen: kan het huidige wettelijke kader adequaat invulling geven aan de behoefte tot aftappen van de behoeftestellers in het licht van de ontwikkelingen?

[1] Met behoeftestellers worden die overheidsinstanties aangeduid die de bevoegdheid hebben om telecommunicatie te onderscheppen, voor de opsporing van strafbare feiten (Openbaar Ministerie, politie) of voor de bescherming van de nationale veiligheid (inlichtingen- en veiligheidsdiensten, ivd's).
[2] *Kamerstukken II* 1995/96, 24 679, nr. 1
[3] In dit rapport korten we gemakshalve 'wet- en regelgeving' vaak af tot 'wetgeving'.

3. Indien de beleidsuitgangspunten of de huidige wet- en regelgeving onvoldoende zijn toegesneden op de gesignaleerde telecommunicatieontwikkelingen, welke oplossingen zijn dan denkbaar die beter invulling zouden kunnen geven aan de behoeften tot aftappen van de behoeftestellers, met inachtneming van de belangen van aanbieders?

1.2. Afbakening, methoden en beperkingen van onderzoek

Dit evaluatieonderzoek beperkt zich tot de hoofdlijnen van het aftapbaarheidsbeleid. Het beleid en de daarop gebaseerde wetgeving kennen veel onderdelen, die soms tot in grote mate van detail zijn uitgewerkt. Wij beperken ons grotendeels tot de drie belangrijkste pijlers van het beleid en de wetgeving, te weten de algemene verplichting dat openbare telecommunicatie aftapbaar moet zijn, de meewerkplichten voor telecomaanbieders, en de kostenverdeling. De overige onderdelen komen slechts kort aan bod. Bovendien gaan wij niet in op de details, zoals van de technische eisen die zijn uitgewerkt in ministeriële regelingen en van de technische specificaties voor overdracht van afgetapte signalen, die voor een beleidsevaluatie niet relevant zijn.
Wij besteden in het toekomstgedeelte van de evaluatie aandacht aan vele technische ontwikkelingen, maar we hebben ons daarbij beperkt tot die ontwikkelingen die voor de kern van de telecommunicatiesector relevant zijn. Meer perifere onderwerpen, zoals satellietcommunicatie, *ambient networking* of *ubiquitous computing*, en RFID zijn daarom niet betrokken bij het onderzoek.[4]
Een volgende beperking in dit onderzoek is dat wij gekozen hebben voor een kwalitatieve, en geen kwantitatieve, evaluatie. De voor het onderzoek beschikbare middelen waren niet toereikend om kwantitatieve gegevens te verzamelen en te analyseren, zoals de financiële administratie van aanbieders om geïnvesteerde kosten voor aftapbaarheid te achterhalen of dossiers van opsporingszaken om technische problemen bij de uitvoering van taps in kaart te brengen. Eveneens was er binnen dit onderzoek geen ruimte voor rechtsvergelijking. Een vergelijking met de situatie in het buitenland is zeker relevant voor de evaluatie van de Nederlandse wetgeving, maar een adequate rechtsvergelijking vergt substantieel onderzoek, niet alleen naar de regeling van aftapbaarheid zelf in andere landen, maar ook naar het systeem van de wet, de plaats van aftappen in het geheel van opsporingsbevoegdheden, en de algemene verdeling van verantwoordelijkheden tussen overheid en private partijen.[5] Voor een dergelijk onderzoek was helaas evenmin ruimte.
Gegeven deze beperkingen, is gekozen voor een kwalitatief onderzoek bestaande uit interviews, aangevuld met literatuuronderzoek. In de periode november 2004 – april 2005 hebben vraaggesprekken plaatsgevonden met de behoeftestellers (Openbaar Ministerie, justitie, politie, AIVD, MIVD), een selectie van aanbieders, de betrokken toezichthouders (OPTA, Agentschap Telecom, CBP) en enkele deskundigen; een volledige lijst van geïnterviewde instanties en personen is te vinden in bijlage IV. De behoeftestellers zijn beperkt in aantal, zodat deze allemaal, gezamenlijk, konden worden geïnterviewd. Voor de aanbieders moest een keuze worden gemaakt. Aangezien het om een kwalitatieve evaluatie gaat, is gekozen voor een selectie van negen grotere en kleinere aanbieders, waarvan sommigen op meerdere markten actief zijn, en die aldus een redelijke afspiegeling vormen van de breedte van de telecommunicatiesector, zonder te streven naar representativiteit. Om deze reden ook worden in het rapport de uitspraken van aanbieders niet gekwantificeerd (“vier van de vijf Internetaanbieders zeggen”) maar slechts in globale zin aangeduid (“sommige aanbieders vinden”, “diverse kleine aanbieders noemen”). In het algemeen hebben wij ook, vanwege de gevoeligheid van het onderwerp, de weergave van meningen geanonimiseerd, tenzij het om een specifieke instantie gaat waarvan het essentieel is dat juist deze instantie het zegt.

[4] Wat de selectie van onderwerpen betreft is het ook goed om te bedenken dat er altijd een (kleine) groep gebruikers is die zich bewust is van het risico afgetapt te worden en die koste wat kost wil voorkomen dat de overheid bepaalde berichten onderschept. Deze groep zal daar – mits zorgvuldig uitgevoerd – meestal in kunnen slagen: door technische bescherming (vercijfering, satelliettelefoons), door slimme trucjes (voor elk gesprek een nieuwe vooruitbetaalkaart) of door het veranderen van gedrag (bijvoorbeeld helemaal af te zien van het gebruik van een telefoon). Dit vraagstuk speelt echter al zo lang als aftappen bestaat en we richten ons bij dit onderzoek dan ook niet specifiek op deze groep gebruikers. We bekijken de invloed van technische ontwikkelingen op de mogelijkheden tot het aftappen van de veel grotere groep 'normale' gebruikers, en op de technieken en diensten die gemeengoed zijn of die dat vermoedelijk zullen worden.

[5] Een indicatie van de situatie in het buitenland is te vinden in Franz Büllingen & Annette Hillebrand, *Rechtlicher Rahmen für das Angebot von TK-Diensten und den Betrieb von TK-Anlagen in den G7-Staaten in Bezug auf die Sicherstellung der Überwachbarkeit der Telekommunikation*, Bad Honnef: wik-Consult, April 2003, en Stratix & Norton Rose, *Inventarisatie regelgeving aftappen in het buitenland*, Schiphol, maart 2004, <http://www.onderzoeksdatabank.minez.nl/rapporten/Rapport.aspx?rapportId=269> (over Duitsland, Frankrijk, Oostenrijk en VK).

Het literatuuronderzoek bestond uit bestudering van relevante wet- en regelgeving, onderzoeksrapporten, beleidsnota's en standpuntnotities over aftapbaarheid, en uit literatuur, hoofdzakelijk via Internet, over ontwikkelingen in de telecommunicatie.
Op basis van deze bronnen kunnen uitspraken worden gedaan ter beantwoording van de onderzoeksvragen. Deze uitspraken kennen twee beperkingen. In de eerste plaats zijn de bevindingen uit de vraaggesprekken gekleurd door de grote belangen die de betrokken partijen hebben bij aftapbaarheid – en dus ook bij de uitkomsten van dit onderzoek. Voor de behoeftestellers is aftappen een essentiële methode om misdadigers en staatsgevaarlijke personen op te sporen, en zij hebben daarom veel belang bij een zo omvangrijk mogelijke verplichte aftapbaarheid. Voor aanbieders is de aftapbaarheidswetgeving een verplichting die veel energie en kosten vergt zonder directe baten, en zij hebben daarom veel belang bij een minimale verplichte aftapbaarheid. De onderzoekers zijn zich bij de gesprekken bewust geweest van deze mogelijke kleuring van de gesprekken en hebben gepoogd deze, tijdens de gesprekken en achteraf bij de analyse, waar mogelijk uit te filteren, onder andere door confrontatie van de uitspraken van de wederzijdse partijen met elkaar. Vanwege de politieke beladenheid van het onderwerp en het debat dat over deze evaluatie zal worden gevoerd, hebben wij er daarbij voor gekozen om, waar het controversiële punten betreft, de behoeftestellers en de aanbieders apart aan het woord te laten en expliciet onderscheid te maken tussen wat de partijen afzonderlijk zeggen en wat wij als onderzoekers, op basis van hun uitspraken maar ook op basis van eigen verworven inzichten, concluderen. De bevindingen van het onderzoek bevatten daarom voor een belangrijk deel de meningen van behoeftestellers en aanbieders, terwijl de conclusies en aanbevelingen voor onze rekening komen.
Een tweede beperking in de resultaten is dat wij sommige bevindingen en conclusies noodzakelijkerwijs algemeen, en soms bewust vaag, formuleren, in verband met de gevoeligheid van deze bevindingen voor de opsporing en staatsveiligheid. Waar bijvoorbeeld het rapport aangeeft dat een deel van de telecommunicatie niet volledig aftapbaar is, kan niet concreet en specifiek aangeduid worden welke netwerken of diensten dan precies niet aftapbaar zijn. Hoewel wij vermoeden dat de meeste berekenende misdadigers en terroristen een goed beeld hebben van wat technisch wel en wat niet aftapbaar is, is het onwenselijk om deze informatie te specificeren omdat dan ook de minder berekenende misdadigers en staatsgevaarlijke personen die informatie zouden kunnen gebruiken om niet-aftapbaar te communiceren.

Het onderzoek is ondersteund door een begeleidingscommissie, die de onderzoeksopzet, tussenrapportages en het eindrapport heeft beoordeeld op inhoudelijke aspecten, kwaliteitsaspecten en aanbevelingen. De onderzoekers danken de leden van de begeleidingscommissie hartelijk voor de constructieve adviezen en commentaren. Het onderzoek is uitgevoerd in de periode november 2004 – juni 2005. Het rapport is afgerond op 21 november 2005.

1.3. Opzet

Dit rapport is als volgt opgebouwd. We beginnen in deel I met een historisch overzicht van het beleid en de wetgeving rond aftapbaarheid tot nu toe (hoofdstuk 2). Vervolgens geven wij in deel II de bevindingen van het eerste deel van de evaluatie, gericht op verleden en heden, door een overzicht van de stand van zaken rond elke pijler van het aftapbaarheidsbeleid: de algemene verplichting dat openbare telecommunicatie aftapbaar moet zijn (hfd. 3), de meewerkplichten voor telecomaanbieders (hfd. 4), en de kostenverdeling (hfd. 5), gevolgd door overige relevante onderwerpen (hfd. 6). Aansluitend volgt in deel III het tweede deel van de bevindingen, gericht op de toekomst, dat een overzicht biedt van ontwikkelingen in telecommunicatie – techniek, markt en identificatiemechanismen – die de aftapbaarheid nu en in de toekomst onder druk kunnen zetten (hfd. 7). Deel IV bevat ten slotte de eigenlijke evaluatie, met een antwoord op de onderzoeksvragen naar de afdoendheid van het beleid (hfd. 8) en naar mogelijke oplossingen voor gesignaleerde tekortkomingen (hfd. 9).
In bijlagen zijn opgenomen de beleidsvoornemens uit 1996, hoofdstuk 13 TW uit 1998 waarin die beleidsvoornemens zijn geïmplementeerd, en hoofdstuk 13 TW zoals geldend op 1 juli 2005.

Deel I. Verleden: achtergronden en geschiedenis

2. Overzicht van beleid en wetgeving

2.1. Technische context

De aftapbaarheid van telecommunicatie wordt in belangrijke mate beïnvloed door technische en marktontwikkelingen. Het is daarom zinvol het beleid te plaatsen tegen de achtergrond van de telecommunicatieontwikkelingen in het verleden die geleid hebben tot het aftapbaarheidsbeleid dat in dit hoofdstuk wordt geschetst. Dit betreft de periode tot ongeveer eind jaren 1990.

In veel opzichten was de telecommunicatiesector in het verleden een betrekkelijk stabiel en weinig veranderlijk veld. Dit geldt zeker voor de periode tot grofweg begin jaren negentig. Alle diensten werden – van overheidswege – door slechts één partij aangeboden, die meestal bekend stond als de nationale PTT. Wat het dienstenaanbod betreft was er weinig veranderd gedurende tientallen jaren. Spraaktelefonie was in alle opzichten de belangrijkste dienst. Hoewel er op technisch vlak wel het een en ander gebeurde (zoals de ontwikkeling en gebruik van de fax, het automatiseren en later digitaliseren van de telefooncentrales, de komst van datatransport en de voorzichtige introductie van autotelefonie). Toch waren de gevolgen hiervan relatief beperkt. De belangrijkste uitdagingen en vraagstukken voor de PTT's gedurende de periode tot aan de jaren tachtig was hoe men de groei van de vraag naar spraaktelefonie wist op te vangen. De uitdaging was om tegen acceptabele kosten alle Nederlandse huishoudens een telefonieverbinding te kunnen bieden, ook als ze op minder gunstige locaties gevestigd waren. Daar waar het gaat om de mogelijke aftapbaarheid van netwerken, bestonden er in die periode weinig knelpunten.
In de periode tussen 1990 en 2000 begon daar verandering in te komen. Veelal waren deze veranderingen het gevolg van beleidsaanpassingen en technische ontwikkelingen die in de jaren tachtig vorm begonnen te krijgen. We vermelden de volgende ontwikkelingen.

- De toename van het aantal marktpartijen: met name als gevolg van Europese regelgeving zijn stapsgewijs steeds meer (deel)markten in het veld van de telecommunicatie aan mededinging blootgesteld. Richtlijn 90/388/EEG uit juni 1990 betrof de opheffing van speciale en exclusieve rechten in deze sector, maar kende nog een aantal belangrijke uitzonderingen, waaronder spraaktelefonie, mobiele diensten en infrastructuur. Stapsgewijs zijn deze uitzonderingen door latere richtlijnen opgeheven: richtlijn 96/2/EG van januari 1996 liberaliseerde mobiele en persoonlijke telecommunicatie, en richtlijn 96/19/EG van maart 1996 bepaalde uiteindelijk dat lidstaten per 1 januari 1998 de gehele telecommunicatiemarkt moesten hebben geliberaliseerd.
- De brede introductie van nieuwe netwerken en diensten, waaronder mobiele telefonie.
- Het toenemend belang van Internet, onder meer door de groeiende populariteit van het World Wide Web.

In het midden van de jaren negentig speelde er dus een aantal ontwikkelingen. Deze waren niet acuut problematisch voor het aftappen door behoeftestellers, omdat vaste telefoniediensten zonder problemen af te tappen bleven, en omdat ondanks de liberalisering het marktaandeel van de voormalige monopolist in bijna alle deelmarkten zeer hoog bleef. Maar naarmate het belang van nieuwe diensten, zoals GSM-telefonie, toenam en het marktaandeel van nieuwe aanbieders steeg, dreigde aftappen minder goed mogelijk te worden. Dit gaf aanleiding tot het ontwikkelen van beleid en wetgeving om aftapbaarheid zeker te stellen.

2.2. Resolutie Europese Raad

Het Nederlandse aftapbaarheidsbeleid moet mede worden gezien in de context van een resolutie van de Europese Raad van 17 januari 1995. De gezamenlijke Ministers van Justitie en Binnenlandse Zaken namen een resolutie aan die de lidstaten verzoekt hun verantwoordelijke telecomministers op te roepen om samen te werken met de justitie- en BiZa-ministers teneinde wetgeving door te voeren die aftapbaarheid van de telecominfrastructuur verplicht stelt.[6]

[6] Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01), *OJ* 4 November 1996, beschikbaar op <http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html> en via <http://www.gliif.org/LI_legal/EU.htm>.

EU Resolution 96/C329/01 (1995)

1. The Council notes that the requirements of Member States to enable them to conduct the lawful interception of telecommunications, annexed to this Resolution ('the Requirements'), constitute an important summary of the needs of the competent authorities for the technical implementation of legally authorized interception in modern telecommunications systems.

2. The Council considers that the aforementioned Requirements should be taken into account in the definition and implementation of measures which may affect the legally authorized interception of telecommunications and requests Member States to call upon the Ministers responsible for telecommunications to support this view and to cooperate with the Ministers responsible for Justice and Home Affairs with the aim of implementing the Requirements in relation to network operators and service providers.

De resolutie bevat een bijlage met eisen van opsporingsdiensten voor het (kunnen) onderscheppen van telecommunicatie. Deze eisen komen grotendeels overeen met (en zijn wellicht geïnspireerd door) wetgeving van de VS, de Communications Assistance for Law Enforcement Act (CALEA)[7] van 1994.[8] Interessant is overigens dat de resolutie volgens één bron tot stand zou zijn gebracht op initiatief van Nederland.[9]

De resolutie is lange tijd met de nodige geheimzinnigheid omgeven. Pas in november 1996 werd de tekst gepubliceerd in het *Official Journal*. Publieke discussie erover vond nauwelijks plaats, zoals vaak het geval is bij besluitvorming in de derde pijler[10].
De resolutie legt strikt genomen geen plicht op aan lidstaten tot aftapbaarheid. De lidstaten worden *verzocht* hun telecommunicatieministers *op te roepen* het document te *ondersteunen* en *samen te werken* met de justitie- en BiZa-ministers. Aan de telecommunicatieministers wordt daarmee (in elk geval letterlijk gezien) een beoordelingsmarge gelaten om te bepalen in hoeverre zij de aftapbaarheidseisen ondersteunen.

2.3. Overzicht van Nederlands beleid en wetgeving

Het aftapbaarheidsbeleid bestaat uit diverse onderdelen en heeft geleidelijk vorm gekregen. Veel aspecten van aftapbaarheid werden aanvankelijk verspreid ontwikkeld binnen de Wet op de telecommunicatievoorzieningen (Wtv), die op 1 januari 1989 in werking trad.[11] Art. 64 Wtv bevatte een verplichting voor de concessiehouder (KPN) om mee te werken met een bevoegd gegeven last tot aftappen.
De volgende stap betrof de invoering van vergunningen voor mobiele telecommunicatie in 1994. Vergunninghouders kregen de verplichting technische aftapbaarheid zeker te stellen en de plicht mee te werken met aftaplasten.[12] Toen vervolgens bleek dat het aftappen van GSM investeringen vergde om de systemen aftapbaar te maken, werd in 1995 bepaald dat de investerings-, exploitatie- en onderhoudskosten voor het aftapbaar maken van het systeem ten laste van de vergunninghouder komen.[13]
Met deze mobieletelecomwetten werd een voorschot genomen op algemene beleidsregels, die in 1996 werden geformuleerd in een *Beleidsvoornemen bevoegd aftappen telecommunicatie*.[14] Dit had de vorm van negen beleidsvoornemens, die later grotendeels zijn uitgevoerd in wet- en regelgeving.
Het *Beleidsvoornemen* is het centrale document dat het beginsel van aftapbaarheid voor de Nederlandse telecommunicatie vastlegt. Redenen om dit beleid te formuleren waren:

- 'de liberalisering en internationalisering van de telecommunicatie;

[7] Zie <http://www.askcalea.net/>.
[8] Op 29-30 november 1993 nam de JBZ-Raad een resolutie aan die tot strekking had de vereisten voor aftapbaarheid van de lidstaten te vergelijken met die van de FBI. Een intentieverklaring (*Memorandum of Understanding*) die aan derde landen werd toegestuurd om de aftapvereisten te onderschrijven, gaf als contactadressen de directeur van de FBI en de secretaris-generaal van de Europese Raad. Aldus Statewatch, *European Union and FBI launch global surveillance system*, februari 1997, <http://www.privacy.org/pi/activities/tapping/statewatch_tap_297.html>. De eisen zijn overigens ook vrijwel gelijkluidend aan de vereisten die zijn vastgesteld door ILETS, het International Law Enforcement Telecommunications Seminar. Zie <http://cryptome.org/ilets-snoop.htm>.
[9] Volgens Statewatch 1997, a.w., noot 8.
[10] De derde pijler van de Europese Unie betreft politie- en justitiezaken, waarbij besluiten worden genomen door de Raad van Ministers en waarbij het Europees Parlement een ondergeschikte rol heeft.
[11] Wet van 26 oktober 1998 (Wet op de telecommunicatievoorzieningen), Stb. 1988, 520, inwerkingtreding 1 januari 1989, Stb. 1988, 550.
[12] Wet van 16 juni 1994 (mobiele telecommunicatie), Stb. 1994, 628.
[13] Wet van 23 november 1995 (aftappen van GSM), Stb. 1995, 594.
[14] *Kamerstukken II* 1995/96, 24 679, nr. 1.

- de snelheid waarmee nieuwe en complexe vormen van telecommunicatie ter beschikking komen van het publiek;
- een toenemende diversiteit van partijen met legitieme, doch op onderdelen tegenstrijdige belangen;
- de stijging van de voor het aftappen noodzakelijke investeringen en andere kosten.'[15]

In het beleidsvoornemen werd teruggegrepen op het precedent van de GSM-wet, maar vooral op de EU-resolutie. Het document geeft aan dat de Raadsresolutie een belangrijke samenvatting geeft van de behoeften van justitie en veiligheidsdiensten, waarmee lidstaten rekening moeten houden; deze 'bepalingen (of vereisten) gelden onverminderd het nationale recht en dienen overeenkomstig de vigerende nationale bepalingen (van de Lidstaten) te worden uitgelegd.' De Minister presenteert de Raadsresolutie daarbij als bindend, feitelijk zonder beoordelingsmarge voor de lidstaten: 'In Denemarken, Duitsland, Ierland, Frankrijk en het Verenigd Koninkrijk is de tenuitvoerlegging van de vereisten in volle gang, al dan niet gepaard met een wijziging van nationale wetgevingen. Een aantal kleinere Lidstaten onderzoekt nog hoe hun nationale wetgevingen moeten worden aangepast om aan de vereisten van de resolutie te kunnen beantwoorden'.[16] Het eerste, centrale voornemen luidt dan ook: 'Wij zullen de vereisten (…) als beleidsuitgangspunten (doen) hanteren voor de invulling van nationale wettelijke aftapregelingen', aldus **voornemen 1**.[17]

Vanuit dit voornemen worden, mede met het oog op de reeds totstandgekomen wetgeving rond GSM, zes voornemens geformuleerd, die neerkomen op beleidsuitgangspunten (zie Bijlage 1 voor de volledige tekst). In het navolgende zullen we dan ook 'beleidsuitgangspunt' als synoniem hanteren voor 'beleidsvoornemen'.

Voornemen 2. Alle publieke telecommunicatienetwerken en -diensten moeten vanaf het moment van introductie aftapbaar zijn.

Voornemen 3. Ook dienstenaanbieders moeten meewerken met aftappen en gegevenslevering.

Voornemen 4. Telecommunicatieaanbieders moeten een adequaat beveiligingsregime inrichten.

Voornemen 5. De investerings-, exploitatie- en onderhoudskosten voor aftapbaarheid en beveiliging komen ten laste van de aanbieders.

Voornemen 6. De kosten voor tapkamers, aftaplijnen en de kosten voor individuele taps komen ten laste van de overheid.

Voornemen 7. De overheid betaalt de helft van de geschatte kosten, NLG 2,9 miljoen, voor het aftapbaar maken van bestaande systemen.

Daarnaast worden nog twee problemen gesignaleerd die nader onderzocht zouden worden:

Voornemen 8. Onderzoek naar de problematiek van informatievoorziening in het licht van de toenemende hoeveelheid aanbieders.

Voornemen 9. Onderzoek naar een informatieplicht ten behoeve van de BVD en de 'dealer-problematiek'. Met dit laatste wordt bedoeld dat er problemen in identificatie kunnen ontstaan doordat consumenten contact hebben met 'dealers' van randapparaten of abonnementen die niet onder de wet vallen, in plaats van met wel aanspreekbare telecomaanbieders.

De beleidsvoornemens zijn, na een algemeen overleg over het document in het parlement,[18] vervolgens uitgevoerd, grotendeels door implementatie in hoofdstuk 13 van de Telecommunicatiewet, die de Wtv in 1998 verving, en door onderliggende besluiten en regelingen.[19] Tabel 1 geeft een overzicht van welk voornemen waarin is geïmplementeerd.

Beleidsvoornemen	Implementatie in	Behandeld in dit rapport
1. vereisten uit EU-resolutie	13.1 lid 2 TW Besluit aftappen, Stb. 1998, 642 Regeling aftappen, Stcrt. 2001, 107	par. 2.4, hfd. 3

[15] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 7.
[16] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 7.
[17] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 8.
[18] Zie *Kamerstukken II* 1995/96, 24 679, nr. 3.
[19] Wet van 19 oktober 198 (Telecommunicatiewet), Stb. 1998, 610.

Beleidsvoornemen	Implementatie in	Behandeld in dit rapport
2. technische aftapbaarheid	13.1 TW 13.7 TW (*) Besluit aftappen, Stb. 1998, 642 Regeling aftappen, Stcrt. 2001, 107	par. 2.4, hfd. 3
3. dienstaanbieders	13.1 TW 13.2 lid 2 TW	par. 2.4, hfd. 3; par. 2.5, hfd. 4
4. beveiliging	13.5 TW Besluit beveiliging gegevens aftappen, Stb. 2003, 472	par. 2.7.1, par. 6.1
5. investeringskosten voor aanbieders	13.6 lid 1 TW	par. 2.6, hfd. 5
6. variabele kosten voor overheid	13.6 lid 2 TW Regeling kosten aftappen en gegevensverstrekking, Stcrt. 31 maart 2005, p. 16	par. 2.6, hfd. 5
7. eenmalige tegemoetkoming	--	par. 2.6, hfd. 5
8. informatievoorziening	13.4 TW	par. 2.5, hfd. 4
9a. meewerkplicht t.b.v. BVD	13.2a TW 13.4 TW *zie ook art. 29 Wiv 2002*	par. 2.5, hfd. 4
9b. 'dealer-problematiek'	13.4 lid 2 en lid 3 TW Besluit bijzondere vergaring nummergegevens, Stb. 2002, 31	par. 2.5, hfd. 4

Tabel 1. Verwijstabel beleidsvoornemens en implementatie
(*) nog niet in werking

Een groot deel van de implementatie vond plaats door inwerkingtreding van de Telecommunicatiewet op 15 december 1998, maar diverse onderdelen zijn pas in een later stadium van kracht geworden na verschijning van algemene maatregelen van bestuur en ministeriële regelingen. Hoofdstuk 13 TW is sinds 1998, op marginale wijzigingen na, niet meer aangepast, ook niet bij de ingrijpende herziening van de Telecommunicatiewet in 2004 waarbij de wet verbreed werd van 'telecommunicatie' naar 'elektronische communicatie' en aldus ook omroepnetwerken en -diensten omvat.[20] Hoofdstuk 13 spreekt dus, in afwijking van de meeste bepalingen uit de TW, nog steeds van openbare telecommunicatienetwerken en -diensten, waaronder omroepnetwerken en -diensten niet vallen.

In de volgende paragrafen gaan we, in iets andere volgorde en groepering, nader in op de diverse onderdelen van het aftapbaarheidsbeleid en de aftapbaarheidswetgeving.

2.4. Uitgangspunt: "Openbare telecommunicatie is aftapbaar"

2.4.1. Technische aftapbaarheid

De belangrijkste pijler van het aftapbaarheidsbeleid is de verplichting voor aanbieders van openbare telecommunicatie om hun netwerken en diensten technisch aftapbaar te maken en te houden.
De eerste aanzet hiervoor werd gegeven bij de invoering van vergunningen voor mobiele telecommunicatie in 1994. In een nieuw hoofdstuk in de Wtv over vergunningen voor specifieke vormen van openbare mobiele telecommunicatie werd een art. 13g opgenomen. Bij AMvB konden regels worden gesteld over verplichtingen waaraan vergunninghouders moesten voldoen; de technische aftapbaarheid was een van die verplichtingen, aldus art. 13g lid 1 onder a Wtv.[21]

Art. 13g Wtv (1994)

[20] Wet van 22 april 2004, Stb. 2004, 189.
[21] Wet van 16 juni 1994 (mobiele telecommunicatie), Stb. 1994, 628.

> 1. (…) Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot de overige verplichtingen van de houder van een vergunning [voor mobiele telecommunicatie]. Deze betreffen:
>
> a. de capaciteit, kwaliteit en eigenschappen, waaronder de **technische aftapbaarheid**, van de telecommunicatie-infrastructuur, bedoeld in artikel 13a, eerste lid (…)

En passant introduceerde de minister hierbij ook de Europese Raadsresolutie: 'Door de Europese Unie zijn reeds begin dit jaar algemene aftapvereisten geformuleerd in een in januari van dit jaar vastgestelde, maar nog niet gepubliceerde Resolutie Aftappen Telecommunicatie. De Europese lidstaten bekijken thans hoe deze vereisten worden geïmplementeerd, door omzetting in nationale wet- en regelgeving.'[22]

Het uitgangspunt van technische aftapbaarheid werd vervolgens in 1996 geformuleerd voor alle publieke telecommunicatienetwerken en -diensten:[23]

> **Beleidsvoornemen 2 (1996)**
>
> Alle telecommunicatienetwerken en -diensten, welke bestemd en toegankelijk zijn voor het algemene publiek, dienen (vanaf het moment van introductie) aftapbaar te zijn.

Het beleidsvoornemen werd uitgewerkt bij de vervanging van de Wtv door de Telecommunicatiewet van 1998. De aftapbaarheidsverplichting, die in het parlement niet ter discussie stond, werd in de wet vastgelegd in nagenoeg dezelfde bewoordingen:[24]

> **Art. 13.1 TW (1998)**
>
> 1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.
>
> 2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

De vereisten van aftapbaarheid zijn nader vastgelegd in een AMvB, het Besluit aftappen openbare telecommunicatienetwerken en -diensten, dat weer is uitgewerkt in een ministeriële regeling.[25] Deze laatste regeling vertaalt de EU-raadsresolutie in technische eisen. Art. 20.13 TW regelde overigens ontheffing van de aftapbaarheidsplicht voor bestaande, nog-niet-aftapbare netwerken en diensten voor een periode van negen maanden na inwerkingtreding van de Telecommunicatiewet (dus tot 15 september 1999).

Van de aftapbaarheidsplicht is volgens art. 13.8 TW eveneens ontheffing mogelijk in bijzondere gevallen. Dit is relevant geweest voor Internetaanbieders, aan wie op basis van AMvB's tot twee keer toe ontheffing werd verleend van de aftapbaarheidsplicht. Van deze mogelijkheid om ontheffing te vragen hebben 33 Internetaanbieders gebruik gemaakt.[26] Deze ontheffing liep tot 15 april 2001; na die datum waren ook zij verplicht aftapbaar te zijn – iets wat in de praktijk overigens niet werd gerealiseerd[27] maar wat nog enige tijd werd gedoogd. In augustus 2002 is door een aantal Internetaanbieders en de brancheverenigingNLIP de Nationale Beheerorganisatie Internet Providers (NBIP) opgericht, waarbij inmiddels zo'n 25 aanbieders zijn aangesloten; de NBIP heeft een aantal verplaatsbare tapsystemen die bij de leden kunnen worden geplaatst op het moment dat zij een tapbevel ontvangen.[28]

[22] *Kamerstukken II* 1994/95, 24 108, nr. 5, p. 5.
[23] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 14.
[24] Wet van 19 oktober 1998 (Telecommunicatiewet), Stb. 1998, 610.
[25] Besluit van 10 november 1998, Stb. 1998, 642, aangepast bij Besluit van 5 juni 2001, houdende wijziging van het Besluit aftappen openbare telecommunicatienetwerken en -diensten, Stb. 2001, 262; Regeling aftappen openbare telecommunicatienetwerken en -diensten, 30 mei 2001, Stcrt. 2001, 107, p. 20.
[26] Beleidsregels ontheffingsverlening aftapbaarheid Internetdiensten, Stcrt. 1999, 86, p. 9; Beleidsregels ontheffingsverlening aftapbaarheid Internetdiensten, Stcrt. 2000, 133, p. 37.
[27] Zie hierover het antwoord van de Minister van Justitie op Kamervragen van Bakker over aftapvoorzieningen bij Internetproviders, 10 mei 2001, *Kamerstukken II* 2000/01, Aanhangsel Handelingen nr. 1155.
[28] Zie <http://www.nbip.nl/>.

2.4.2. Openbaarheid

De verplichting tot aftapbaarheid geldt alleen aanbieders van *openbare* telecommunicatie. In het beleidsvoornemen werd dit aangeduid als telecommunicatie die 'bestemd en toegankelijk [is] voor het algemene publiek'. Dit wordt nader uitgelegd: 'Bepalend voor «openbaar» is het karakter van het gebruik van de dienst die geleverd wordt. Een dienst is openbaar indien eenieder, zonder onderscheid, er gebruik van kan maken, of zich er op kan abonneren. Een netwerk waarover een openbare dienst wordt geleverd is daarmee ook openbaar.'[29]

In de Telecommunicatiewet werd de term 'openbare telecommunicatie' als volgt uitgelegd:
- '*openbare telecommunicatiedienst*: telecommunicatiedienst die beschikbaar is voor het publiek;
- *openbaar telecommunicatienetwerk*: een telecommunicatienetwerk dat onder meer voor de verrichting van openbare telecommunicatiediensten wordt gebruikt of een telecommunicatienetwerk waarmee aan het publiek de mogelijkheid tot overdracht van signalen tussen netwerkaansluitpunten ter beschikking gesteld wordt' (art. 1.1 onder f en g TW).

De toelichting stelt dat kenmerkend is voor openbaarheid 'het feit dat de betreffende telecommunicatiedienst beschikbaar is voor het publiek. Daarmee wordt bedoeld dat de betreffende dienst openbaar wordt aangeboden en beschikbaar is voor eenieder die van dat aanbod gebruik wil maken tegen de in het openbare aanbod vermelde condities.' Diensten 'die uitsluitend beschikbaar zijn voor leden van een besloten gebruikersgroep' zijn geen openbare telecommunicatiediensten.[30] Wat in dit verband een besloten gebruikersgroep is, wordt niet nader toegelicht in de Memorie van Toelichting;[31] de Nota naar aanleiding van het Verslag geeft aan dat dit hetzelfde begrip is als de gesloten gebruikersgroepen onder de Wtv, waarmee de nodige ervaring is opgedaan.[32]
Sinds de verbreding van de TW in 2004 tot elektronische communicatie, dus inclusief omroep, (zie par. 2.3), worden de volgende definities gehanteerd:
- '*openbaar telecommunicatienetwerk*: elektronisch communicatienetwerk dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden, voor zover het netwerk niet gebruikt wordt voor het verspreiden van programma's;
- *openbare telecommunicatiedienst*: voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het verspreiden van programma's' (art. 1.1 onder ee en ff TW).

In de Telecommunicatiewet wordt ook de mogelijkheid opgenomen om besloten diensten of netwerken onder omstandigheden aftapbaarheidsplichten op te leggen. Deze mogelijkheid is vormgegeven in art. 13.7 TW: 'Onze Minister kan in het belang van de veiligheid van de staat of de handhaving van de strafrechtelijke rechtsorde bij beschikking bepalen dat een of meer artikelen van dit hoofdstuk (...) van overeenkomstige toepassing zijn op aanbieders van een niet-openbaar telecommunicatienetwerk, een niet-openbare telecommunicatiedienst of aanbieders van huurlijnen indien het netwerk, de dienst of een huurlijn feitelijk openstaat voor derden.' (Hierbij wordt wel een alternatieve kostenverdeling, zie par. 2.6, gehanteerd, ingevoegd bij amendement.[33]) Als voorbeeld werd genoemd de situatie waarin een verdachte vanuit een niet-openbaar netwerk naar buiten belt, waarbij dan een meewerkplicht op de netwerkaanbieder kan worden gelegd om te helpen de interne gebruiker af te tappen, zodat niet al het uitgaande netwerkverkeer hoeft te worden getapt.[34]
Aangezien er in 1998 nog geen bevoegdheden bestonden om besloten telecommunicatie te onderscheppen, werd besloten art. 13.7 TW nog niet in werking te laten treden, in afwachting van de Wet bijzondere opsporingsbevoegdheden en de Wiv 2002.[35] Sinds de inwerkingtreding van

[29] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 8.
[30] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 72.
[31] De MvT merkt wel op dat van een besloten groep sprake is 'als er bepaalde kwaliteitseisen worden gesteld, bijvoorbeeld het behoren tot een bepaalde beroepsgroep of bedrijfstak' (p. 55), maar dit heeft betrekking op de besloten groep bij omroep, zoals geregeld in de Mediawet, en niet op telecommunicatiediensten of -netwerken.
[32] *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 6.
[33] *Kamerstukken II* 1997/98, 25 533, nr. 15.
[34] *Kamerstukken I* 1998/99, 25 533, nr. 11a, p. 6.
[35] *Kamerstukken I* 1998/99, 25 533, nr. 11b, p. 9-10.

deze wetten[36] is er echter kennelijk geen aanleiding geweest om de aftapbaarheid van besloten netwerken of diensten af te dwingen: art. 13.7 TW is namelijk ook later niet in werking getreden.

2.4.3. Netwerken én diensten

Zoals het derde beleidsvoornemen uit 1996 al aangaf, geldt de aftapbaarheidsverplichting zowel voor netwerken als voor diensten. 'Omdat in de moderne systemen ook dienstenleveranciers ten behoeve van hun dienstvoorziening schakelmiddelen kunnen exploiteren dient de aftapbaarheid zich niet te beperken tot de (kale) netwerken. Het is niet uitgesloten dat ook de dienstenleveranciers technische tapfaciliteiten zullen moeten plaatsen.'[37] Naarmate er meer diensten komen van uiteenlopende aanbieders, is het aftappen van het netwerk minder aantrekkelijk: een tap levert dan immers grote hoeveelheden ruwe data op die moeten worden geïnterpreteerd en waaruit ook nog de specifieke gegevens van de bewuste dienst moeten geselecteerd. Het feit dat dan wel taps bij diverse dienstenaanbieders moeten worden geplaatst, wat extra inspanningen vergt, wordt daarbij dan voor lief genomen.
De keuze om de verplichtingen voor technische aftapbaarheid zowel aan netwerk- als aan dienstaanbieders op te leggen, wordt summier toegelicht bij de behandeling van de Telecommunicatiewet. De Memorie van Toelichting herhaalt slechts letterlijk de bovengeciteerde passage uit het beleidsvoornemen.[38] Later wordt nog als extra argument gegeven dat aanbieders nodig zijn 'voor het verstrekken van informatie om daarmee de aftaplast überhaupt te kunnen invullen',[39] wat ons overigens geen argument lijkt om dienstaanbieders te verplichten om technische aftapbaarheid van hun dienst te verzekeren.

2.4.4. Transmissieprotocollen

Een essentieel onderdeel van de aftapbaarheid is dat door aanbieders onderschepte signalen op de juiste wijze naar de behoeftestellers worden geleid. Hiervoor zijn afspraken nodig die vastleggen welke technische specificaties de aanbieder moet hanteren voor de doorgifte van tapsignalen. Voor het aftappen van spraakverkeer, zowel vast als mobiel, is in Nederland daarvoor het zogenoemde ETSI-NL-protocol ontwikkeld. Dit protocol beschrijft in detail hoe de communicatie van het afgetapte verkeer tussen de aanbieder en de behoeftesteller verloopt.[40] De behoefte aan dergelijke technische afspraken speelt natuurlijk in meerdere landen, en de naam van dit protocol geeft reeds aan dat het hier gebruikte protocol aanleunt tegen een techniek die door het Europese normalisatie-instituut ETSI (European Telecommunications Standards Institute) is vastgesteld. Om te voldoen aan enkele bijzondere eisen die in de Nederlandse context werden gesteld en om de norm nader in te vullen, is er een Nederlandse variant (of aanvulling) opgesteld; vandaar de naam ETSI-NL.[41] Hier moet opgemerkt worden dat ook andere landen specifieke varianten kunnen hanteren.
Voor Internet- en e-mail-taps moest een ander protocol worden ontwikkeld voor de uitwisseling van de tapgegevens tussen aanbieder en behoeftesteller. Omdat Nederland met deze ontwikkeling voor liep op andere landen, is een eigen *hand-over*-protocol ontwikkeld. Dat staat bekend onder de naam TIIT (Transport of Intercepted IP Traffic).[42] In ETSI wordt overigens momenteel ook aan een dergelijk (internationaal) protocol voor Internetverkeer gewerkt; uit de vraaggesprekken bleek echter dat deze ontwikkeling sterk lijkt vertraagd en dat de meningen verdeeld zijn of die ontwikkeling veel kans op succes maakt.

[36] De Wet BOB (Stb. 1999, 245) trad in werking op 1 februari 2000 (Stb. 2000, 32), de Wiv 2002 (Stb. 2002, 148) op 29 mei 2002 (Stb. 2002, 196).
[37] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 8.
[38] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 124.
[39] *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 136.
[40] Een dergelijk protocol wordt daarom ook wel als een 'hand-over'-protocol aangeduid. Het betreft immers het overdragen van de gegeven van de ene partij aan de andere. Let wel: dat is iets anders dan het bekende begrip *hand-over* uit de mobiele telecommunicatie, waar dat begrip wordt gebruikt voor het schakelen van een gesprek van het ene naar het andere basisstation.
[41] ETSI-NL bouwt voor op ETSI ES 201 671: *Handover interface for the lawful interception of telecommunication traffic*, version 1.1.1 (1999-07). De meest bijzondere aanpassing voor de Nederlandse context betreft het gebruik van zogenaamde subadressering die gebruikt wordt voor bepaalde authenticatie.
[42] Working group TIIT Bake Off phase 2, *TIIT v.1.0.0 (2002-09), Transport of Intercepted IP Traffic*, The Hague: Ministry of Economic Affairs 2002.

2.5. Meewerkplichten

2.5.1. Meewerken aan aftappen

Naast technische ontwikkelingen is ook de liberalisering van de telecomsector van invloed geweest op de mogelijkheid tot aftappen. Van oudsher was de telefonie een staatsmonopolie, zodat de medewerking van de telefonieambtenaren aan het aftappen op basis van intern-ambtelijke instructies kon plaatsvinden. Met de privatisering van de PTT veranderde dit echter; de medewerkingsplicht moest nu wettelijk worden verankerd.[43] In de Wet op de telecommunicatievoorzieningen werd daartoe een artikel opgenomen:[44]

> **Art. 64 Wtv (1988)**
>
> De houder van de concessie is verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegevene bijzondere last tot het afluisteren of opnemen van telecommunicatie die over de telecommunicatie-infrastructuur wordt afgewikkeld.

Bij de Wet mobiele telecommunicatie werd deze verplichting ook van toepassing verklaard op aanbieders van mobiele telecommunicatie:[45]

> **Art. 64 Wtv (1994)**
>
> 1. De houder van de concessie, onderscheidenlijk de houder van een vergunning, is verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegevene bijzondere last tot het afluisteren of opnemen van telecommunicatie die over de telecommunicatie-infrastructuur wordt afgewikkeld.
>
> 2. Het eerste lid is tevens van toepassing met betrekking tot de telecommunicatie die wordt afgewikkeld over de telecommunicatie-inrichtingen van de houder van een machtiging die de desbetreffende telecommunicatie-inrichtingen gebruikt ten behoeve van het voor derden verzorgen van het transport van gegevens met en tussen mobiele gebruikers.

In de Telecommunicatiewet keerde deze verplichting terug, onderscheiden naar netwerken en diensten:[46]

> **Art. 13.2 TW (1998)**
>
> 1. Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.
>
> 2. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van door hen verzorgde telecommunicatie.
>
> 3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

Deze bepaling is vervolgens aangepast bij de wet Wiv 2002,[47] waarbij is ingevoegd ‘dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002’. Vervolgens is door de Wet vorderen gegevens telecommunicatie[48] de ‘bevoegd gegeven last’ vervangen door ‘een bevel op grond van het Wetboek van Strafvordering’. Opmerkelijk daarbij is dat ‘bevoegd gegeven’ is verdwenen. Een kwaadwillende lezer zou uit deze wijziging kunnen afleiden dat aanbieders nu ook moeten meewerken met onbevoegd gegeven bevelen op basis van Sv of de Wiv, maar dat zal niet de bedoeling van de wetgever zijn. De – niet toegelichte – wijziging heeft vermoedelijk te maken met het voorkomen dat aanbieders in discussie gaan over de bevoegdheid van een gegeven last: zij moeten het bevel gewoon opvolgen (vgl. par. 4.1).

---

[43] ‘Na de verzelfstandiging zal deze medewerking alleen gegeven kunnen worden krachtens een wettelijke verplichting.’ *Kamerstukken II* 1987/88, 20 369, nr. 7, p. 2.
[44] Wet van 26 oktober 1988, houdende regels met betrekking tot voorzieningen voor telecommunicatie (Wet op de telecommunicatievoorzieningen), Stb. 1988, 520. Art. 64 werd ingevoerd bij Nota van Wijziging, *Kamerstukken II* 1987/88, 20 369, nr. 7.
[45] Wet van 16 juni 1994 (…) in verband met de doorbreking van het exclusieve recht van de concessiehouder in hoofdszaak door middel van de invoering van een gelimiteerd vergunningenstelsel voor specifieke vormen van openbare mobiele telecommunicatie (mobiele telecommunicatie), Stb. 1994, 628.
[46] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Stb. 1998, 610.
[47] Stb. 2002, 148.
[48] Stb. 2004, 105.

2.5.2. Meewerken aan verstrekken van verkeersgegevens

Telecomaanbieders moeten niet alleen meewerken aan een last tot aftappen, zij moeten ook voldoen aan vorderingen om verkeersgegevens te verstrekken. Deze verplichting was tot voor kort echter niet te vinden in de Telecommunicatiewet. Dat wil niet zeggen dat aanbieders straffeloos konden weigeren: art. 125f Sv, in 2000 vervangen door art. 126n/u Sv, geeft de officier van justitie de bevoegdheid om bij aanbieders verkeersgegevens op te vragen, en art. 184 Sr kent een algemene strafbepaling voor het niet meewerken aan een bevoegd gegeven ambtelijk bevel. Bij de Wet vorderen gegevens telecommunicatie, die op 1 september 2004 in werking is getreden, is echter ook hiervoor een expliciete verplichting in de TW opgenomen.[49] In de Memorie van Toelichting bij deze wet is overigens niet toegelicht waarom deze verplichting zelfstandig in de TW opgenomen moest worden; er was kennelijk een behoefte aan een spiegelbepaling in de TW.

Art. 13.2a TW (2004)

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126n of artikel 126u van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens over een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst en het telecommunicatieverkeer met betrekking tot die gebruiker.

2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan de vordering of het verzoek voldoen en de wijze waarop de gegevens, bedoeld in het eerste lid, beschikbaar worden gehouden.

2.5.3. Meewerken aan verstrekken van gebruikersgegevens

Anders dan bij verkeersgegevens het geval was, kende de Telecommunicatiewet wel reeds in 1998 een verplichting voor aanbieders om gebruikersgegevens te verstrekken. De verstrekking van gebruikersgegevens werd gezien als een hulpbevoegdheid voor de tap en de vordering tot verstrekken van verkeersgegevens: die bevoegdheden kunnen immers niet worden uitgeoefend als de behoeftestellers niet weten welk aansluitnummer een te onderzoeken persoon heeft. Artikel 13.4 lid 1 TW kwam aldus te luiden: 'Aanbieders (...) zijn verplicht aan de autoriteiten de informatie te verstrekken die noodzakelijk is om die autoriteiten in staat te stellen de (...) bevoegdheden tot het aftappen (...) dan wel tot het vorderen van [verkeersgegevens] te kunnen uitoefenen. Deze verplichting omvat in ieder geval het desgevraagd aan de autoriteiten meedelen van het aan een gebruiker verleende nummer[50] en de door hem afgenomen openbare telecommunicatiedienst, en het desgevraagd aan de autoriteiten meedelen van de bij een nummer behorende naam-, adres-, postcode- en woonplaatsgegevens.'
Bij de inwerkingtreding van de Wet vorderen gegevens telecommunicatie, waarbij voor het eerst een justitiële bevoegdheid tot het vorderen van gebruikersgegevens werd ingevoerd (art. 126na/ua Sv), is de bepaling echter gewijzigd: 'Aanbieders (...) voldoen aan een vordering op grond van artikel 126na, eerste lid, of 126ua, eerste lid, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst (...).'
Aangezien hierbij de koppeling met het mogelijk maken van een tap of vordering verkeersgegevens is verdwenen, wordt de bevoegdheid kennelijk inmiddels gezien als een zelfstandige bevoegdheid. Wel blijft de meewerkplicht beperkt tot het verstrekken van gebruikersgegevens aan justitie ten behoeve van de strafvordering en aan inlichtingen- en veiligheidsdiensten op basis van de Wiv 2002.

2.5.4. Centraal informatiepunt (CIOT)

In 1996 werd gesignaleerd dat door de toenemende hoeveelheid aanbieders het voor behoeftestellers moeilijker zou worden te achterhalen welke telecomaansluitingen een verdachte heeft die afgetapt moet worden of waarvan verkeersgegevens opgevraagd moeten worden. De

[49] Stb. 2004, 105.
[50] In dit rapport wordt het begrip 'nummer', conform art. 1.1 TW, in brede zin gebruikt: 'cijfers, letters of andere symbolen, al dan niet in combinatie, die bestemd zijn voor toegang tot of identificatie van gebruikers, netwerkexploitanten, diensten, netwerkaansluitpunten of andere netwerkelementen'. Het begrip omvat dus ook diverse soorten identiteiten bij Internet.

behoeftestellers zouden dan bij alle aanbieders afzonderlijk moeten navragen of verdachte daar abonnee is.
In dat licht werd beleidsvoornemen 8 opgesteld, waarbij gedacht werd aan een 'centraal informatievoorzieningssysteem van netwerkbeheerders en dienstenleveranciers':[51]

> **Beleidsvoornemen 8 (1996)**
>
> De wettelijk verplichte informatievoorziening door netwerkbeheerders en dienstenleveranciers wordt door de verspreiding van die informatie complex. De problematiek zal worden onderzocht opdat binnen een half jaar ter zake voorstellen gedaan kunnen worden.

Als uitvloeisel van dit voornemen werd in het derde lid van art. 13.4 TW (dat verplichte medewerking bij gebruikersgegevens regelt, zie vorige paragraaf) de mogelijkheid opgenomen om bij algemene maatregel van bestuur regels te stellen 'met betrekking tot de wijze van verstrekking van de informatie, bedoeld in het eerste lid, en de wijze waarop daartoe de gegevens beschikbaar worden gehouden.' De desbetreffende AMvB werd in januari 2000 gepubliceerd: het *Besluit verstrekking gegevens telecommunicatie*, dat overigens pas op 1 september 2004 in werking trad.[52] Hierin werd een nieuwe orgaan, het Centraal informatiepunt onderzoek telecommunicatie (CIOT), geïntroduceerd. Het CIOT is een centrale waaraan telecommunicatieaanbieders iedere 24 uur een geactualiseerd bestand van gebruikersgegevens beschikbaar moeten stellen (art. 3 lid 4 en art. 4 Besluit). Behoeftestellers kunnen geautomatiseerd gebruikersgegevens opvragen aan de hand van een bepaald naam, adres of nummer (art. 3 lid 2 en art. 5 Besluit). Zij kunnen dus bij een bepaalde naam of adres het aansluitnummer opvragen, maar ook aan de hand van een gevonden telefoonnummer een tenaamstelling opvragen. Ongerichte zoekacties (zoals 'bladeren' door alle gegevens van het CIOT) zijn echter technisch onmogelijk. Desgevraagd door een bevoegde autoriteit dienen aanbieders gebruikersgegevens te corrigeren of toe te lichten (art. 3 lid 5 Besluit).
Volgens artikel 11 van het besluit hoeven Internetaanbieders niet mee te werken met het CIOT; deze ontheffing geldt voor een periode twee jaar (art. 12 lid 2 Besluit), dus tot 1 september 2006. Zij mogen overigens wel vrijwillig besluiten om de verstrekkingen van gebruikersgegevens (die ze op basis van de TW toch verplicht zijn te doen), via het CIOT te laten verlopen (art. 11 lid 2).

Ondanks het feit dat het Besluit pas in 2004 formeel in werking trad, is wel eerder informeel uitvoering gegeven aan het CIOT, op basis van afspraken tussen aanbieders en behoeftestellers.

2.5.5. Bewaarplicht i.v.m. vooruitbetaalkaarten

Telecomaanbieders zijn dus verplicht om gebruikersgegevens te leveren. Bij vooruitbetaalkaarten levert dat een probleem op, aangezien de aanbieders daarbij niet (altijd) weten wie gebruik maken van hun netwerken of diensten. De enige oplossing die de overheid aanvankelijk hiervoor kon bedenken, was een registratieplicht: iedereen die een vooruitbetaalde kaart koopt zou zich moeten identificeren met een legitimatiebewijs, waarbij een register zou worden aangelegd. Dit zware (paarden)middel kon achterwege worden gelaten toen er technische oplossingen werden ontdekt. De eerste oplossing was een bestandsanalyse door een telecomaanbieder, waarbij hij door analyse van zijn gegevensbestanden het benodigde aansluitnummer van de mobiele telefoon kan achterhalen. Wanneer justitie de af te tappen persoon op minstens twee verschillende tijdstippen heeft geobserveerd als mobiel bellend, kan zij aan de aanbieder doorgeven op welke tijdstippen op welke locaties door een toestel gebeld is. De aanbieder kan vervolgens in zijn bestand achterhalen welk nummer in al deze gevallen belde. In sommige gevallen (op plaatsen of tijdstippen waar weinig mobiel wordt gebeld, of wanneer justitie weet met wie de persoon belde) kan worden volstaan met één observatie van tijdstip en locatie. Aldus kan de aanbieder veelal in een kwartiertje het gevraagde nummer achterhalen.[53] De tweede mogelijkheid is een IMSI-vanger: een zender die zich als basisstation voordoet om de gezochte mobiele telefoon te lokken (die via observatie in de gaten wordt gehouden) zich aan te melden, waarmee de telefoon automatisch zijn aansluitnummer prijsgeeft. Omdat deze tweede

[51] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 12 en 14.
[52] Besluit van 26 januari 2000 (Besluit verstrekking gegevens telecommunicatie), Stb. 2000, 71. Inwerkingtreding: Besluit van 16 augustus 2004, Stb. 2004, 211.
[53] Zie de toelichting in het *Besluit bijzondere vergaring nummergegevens telecommunicatie*, Stb. 2002, 31, p. 14-15.

mogelijkheid ingrijpt in het normale frequentiegebruik, wordt dit gezien als een zwaardere methode dan de eerste.[54]
In de loop van de Telecommunicatiewetsgeschiedenis werden deze twee oplossingen vastgelegd in de wet, de IMSI-vanger in art. 3.10 lid 4 TW (later aangevuld met een expliciete bevoegdheid in art. 126na/ua Sv)[55], en de bestandsanalyse door telecomaanbieders in art. 13.4 lid 2 TW. Om de bestandsanalyse mogelijk te maken, werd ook een – beperkte – bewaarplicht ingevoerd.

> **Artikel 13.4 lid 2 Telecommunicatiewet (1998)**
>
> 2. Indien de in het eerste lid bedoelde informatie [de gebruikersgegevens] niet bij de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten bekend is, zijn zij verplicht de informatie te achterhalen en te verstrekken op een bij algemene maatregel van bestuur te bepalen wijze. Teneinde aan deze verplichting te kunnen voldoen, bewaren de aanbieders de daartoe benodigde, bij algemene maatregel van bestuur aan te wijzen gegevens, voor een termijn van drie maanden, nadat de gegevens voor het eerst zijn verwerkt.[56]

De bewaarplicht geldt voor 'bij algemene maatregel van bestuur aan te wijzen gegevens'. Deze AMvB is het *Besluit bijzondere vergaring nummergegevens telecommunicatie* uit december 2001 (in werking sinds 1 maart 2002), dat de verplichting tot bestandsanalyse uitwerkt en de hiertoe te bewaren gegevens aanwijst:[57]

> **Art. 7 Besluit bijzondere vergaring nummergegevens telecommunicatie (2002)**
>
> Als gegevens, bedoeld in artikel 13.4, tweede lid, tweede volzin, van de wet, worden aangewezen:
>
> a. de tijdstippen waarop telecommunicatie heeft plaatsgevonden,
>
> b. de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers,
>
> c. bij welk basisstation elk van de gegevens onder a en b zijn binnengekomen.

De bewaarplicht geldt alleen voorzover deze gegevens worden verwerkt door de telecom-aanbieder; hij hoeft ze niet te vergaren als hij ze zelf niet verwerkt. Aanbieders die geen gegevens verwerken over het basisstation hoeven dus niet aan de bewaarplicht en de bestandsanalyseplicht van 13.4 lid 2 TW te voldoen. Volgens de wetgever betreft het evenwel gegevens die veelal nodig zijn voor bedrijfsdoeleinden van de aanbieder, bijvoorbeeld voor fraudebestrijding, het afhandelen van klachten en het verbeteren van de kwaliteit van het netwerk.[58]
Hoewel achtergrond van de bewaarplicht de problematiek van vooruitbetaalde kaarten betreft en dus alleen relevant is voor aanbieders van mobiele telecommunicatie met betrekking tot communicatie die wordt gevoerd met beltegoedkaarten, is in de wet noch in de regelgeving een beperking tot mobiele aanbieders te vinden. Naar de geest van de wet zouden de bepalingen echter wel restrictief moeten worden uitgelegd: de bewaarplicht geldt alleen voor aanbieders van mobiele telecommunicatie.

2.5.6. Algemene bewaarplicht

De huidige bewaarplicht geldt alleen voor vooruitbetaalkaarten bij mobiele aanbieders voor een periode van drie maanden. Sinds enkele jaren wordt er hevig gediscussieerd over de invoering van een veel verderstrekkende bewaarverplichting voor verkeersgegevens. Binnen de EU wordt een kaderbesluit overwogen dat lidstaten zou verplichten bewaring te eisen van alle verkeersgegevens gedurende één tot drie jaar.[59] Daarbij gaat het om de vastlegging en het

[54] Zie over het probleem, de registratieplicht en de technische oplossingen de toelichting in *Kamerstukken II* 1997/98, 25 533, nr. 8, p. 10-12. Merk op dat de IMSI-vanger niet dient om verkeersgegevens te vergaren; het gaat om het verkrijgen van de (NAW- en nummer)gegevens die nodig zijn om verkeersgegevens te kunnen opvragen of een tap te kunnen plaatsen. *Kamerstukken I* 1998/99, 25 533, nr. 11a, p. 4. Het CBP tekent overigens wel aan dat een IMSI-vanger instelbaar is en meer gegevens kan opvangen dan alleen de gebruikersgegevens; het is moeilijk om hierop controle uit te oefenen.
[55] Bij wet van 5 april 2001, Stb. 180.
[56] In de wet vorderen gegevens telecommunicatie, Stb. 2004, 105, is deze bepaling aangepast; de bewaarplicht van de laatste volzin is iets anders geformuleerd maar werd inhoudelijk niet aangepast: 'Teneinde aan deze verplichting te kunnen voldoen bewaren de aanbieders bij algemene maatregel van bestuur aan te wijzen gegevens voor een periode van drie maanden, vanaf het tijdstip waarop deze gegevens voor de eerste maal zijn verwerkt.'
[57] Besluit van 18 december 2001, houdende regels voor de vergaring van nummergegevens door middel van afwijkend frequentiegebruik en bestandsanalyse met het oog op onderzoek van telecommunicatie (Besluit bijzondere vergaring nummergegevens telecommunicatie), Stb. 2002, 31, inwerkingtreding 1 maart 2002 (Stb. 2002, 106).
[58] Besluit bijzondere vergaring nummergegevens telecommunicatie, Stb. 2002, 31, p. 8 en 15.
[59] *Draft Framework Decision on the retention of data (...) for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, 28 april 2004, beschikbaar op

behoud van gegevens die louter voor strafrechtelijke of nationaleveiligheidsdoeleinden moeten worden opgeslagen voor de toekomst. De periode van bewaring en de soorten gegevens zijn nog onder discussie, evenals de vraag of de bewaarplicht alleen zou gelden voor gegevens die de aanbieder toch al voor korte of lange tijd opslaat, of dat er een vergaarplicht zou komen waarbij aanbieders nieuwe gegevens zouden moeten genereren om op te slaan. Daarnaast wordt nu overwogen om de bewaarplicht eerst in te voeren voor telefonie, en later voor Internet. Het is ook nog de vraag of de regeling kan worden getroffen als kaderbesluit (door de Raad van Ministers) of als richtlijn (door de Europese Commissie en het Europees Parlement); de Europese Commissie heeft aangekondigd zelf met een richtlijnvoorstel te komen.[60] Het Nederlandse parlement staat vooralsnog kritisch tegenover (overhaaste invoering van) een bewaarplicht, zoals blijkt uit de op 2 juni 2005 aangenomen motie van de Tweede Kamer en de gedachtewisseling in de Eerste Kamer op 28 juni 2005.[61]
Aangezien beleid en wetgeving rond een algemene bewaarplicht nog in ontwikkeling zijn, wordt deze verder buiten beschouwing gelaten in dit onderzoek.

2.6. Kostenverdeling

2.6.1. Kosten voor aftapbaarheid en operationele kosten

Toen medio jaren ’90 bleek dat het aftappen van GSM investeringen vergde om de systemen aftapbaar te maken, werd in 1995 bepaald dat de investerings-, exploitatie- en onderhoudskosten voor het aftapbaar maken van het systeem ten laste van de vergunninghouder komen.[62]

> **Art. 64a Wtv (1995)**
>
> De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door de houder van een vergunning voor het voor derden verzorgen van openbare mobiele telecommunicatie (…) zijn gemaakt teneinde te kunnen voldoen aan het bepaalde in artikel 64, komen te zijnen laste.

Deze kostenverdeling ligt volgens de minister voor de hand, omdat het ‘hier immers geen kosten [betreft] die direct voortvloeien uit het aftappen zelf, maar kosten die de vergunninghouder moet maken om te voldoen aan de wettelijke vereisten. (…) Daarnaast spelen ook budgettaire overwegingen een rol.’[63] In het laatste kan men tussen de regels door lezen dat de kosten voor het aftapbaar maken en houden van de telecominfrastructuur te hoog worden gevonden om door de staat te laten dragen. De wet beperkt zich tot GSM; de discussie over de kosten van aftapbaarheid van andere netwerken zal bij de herziening van de Wtv aan de orde komen,[64] al kondigt de minister wel reeds aan daarbij dezelfde kostenverdeling voor te zullen stellen.[65]

De kostenverdeling wordt vervolgens voor alle vormen van publieke telecommunicatie uitgewerkt in het *Beleidsvoornemen*. Kosten voor aftapbaarheid zijn voor rekening van aanbieders, kosten voor concrete taps voor rekening van de behoeftestellers.[66]

> **Beleidsvoornemen 5**
>
> De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen in verband met het aftappen en de informatieverstrekking alsmede in verband met de beveiliging zijn ten laste van de netwerkbeheerders respectievelijk de dienstenleveranciers.
>
> **Beleidsvoornemen 6**
>
> De bevoegde instanties blijven de kosten betalen die gepaard gaan met de inrichting van tapkamers, de huur van aftaplijnen en de zogenaamde direkte kosten (i.e. de personeels- en administratiekosten) per

---

<http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>.
[60] Zie voor een overzicht van alle relevante documenten en kritiekpunten op de voorstellen <http://www.bof.nl/verkeersgegevens.html> en het dossier bewaring verkeersgegevens (JBZ-dossier 4.0.6) van de Eerste Kamer op <http://www.europapoort.nl/9345000/1f/j9vvgy6i0ydh7th/vgq8mlyezvzt>.
[61] *Kamerstukken II* 2004/05, 23 490, nr. 372 (zie echter ook de verworpen motie met nr. 373), *Handelingen II* 2 juni 2005, 86-5127/5128; *Handelingen I* 28 juni 2005, ongecorrigeerd verslag beschikbaar op <http://www.europapoort.nl/>. Zie ook het ongedateerde, auteurloze rapport *Wie wat bewaart die heeft wat* van de Erasmus Universiteit Rotterdam, beschikbaar op <http://www.justitie.nl>, aangeboden aan de Tweede Kamer op 20 juni 2005, *Kamerstukken II* 2004/05, 23 490, nr. 379.
[62] Wet van 23 november 1995 (aftappen van GSM), Stb. 1995, 594.
[63] *Kamerstukken II* 1994/95, 24 108, nr. 3, p. 1.
[64] *Kamerstukken II* 1994/95, 24 108, nr. 3, p. 2.
[65] *Handelingen II* 25 oktober 1995, 17-1124.
[66] *Kamerstukken II* 1995/96, 24 679, nr. 1.

> individuele tap of informatieverstrekking. De Minister van Binnenlandse Zaken blijft de kosten voor de veiligheidsonderzoeken betalen.

Bij de toelichting op deze voornemens wordt dezelfde argumentatie als bij de GSM-wet gehanteerd: het gaat om kosten die voortvloeien uit wettelijke verplichtingen en om budgettaire overwegingen. Bij dit laatste wordt aangegeven dat de kosten van tappen voor de Staat stijgen:

> 'Deze kostenstijging wordt enerzijds veroorzaakt doordat opsporingsinstanties bij de bestrijding van de criminaliteit vaker dan voorheen het middel van de telefoontap moeten gebruiken, en anderzijds doordat het afluisterbaar maken van nieuwe vormen van telecommunicatie ook voor de Staat steeds opnieuw investeringen vereist. Daarbij valt bijvoorbeeld te denken aan de aanpassing van de tapkamers. De Staat wordt kortom geconfronteerd met de gevolgen van de technische ontwikkelingen op het gebied van de telecommunicatie in de vorm van steeds hogere rekeningen voor het aftappen.'[67]

Bovendien wijst de beleidsnotitie erop dat het parlement inmiddels reeds heeft ingestemd met deze kostenverdeling voor GSM.[68] Een aspect van de kostenverdeling dat min of meer een eigen leven is gaan leiden, betreft een schatting van de minister van de totale investeringskosten: 'Op de totale investeringskosten is dit naar verwachting slechts een klein percentage (in geval van GSM ruw geschat op ongeveer 1 %).'[69] In antwoord op vragen van de kamercommissie werd deze ruwe schatting voor GSM echter met meer stelligheid geponeerd, en werd bovendien de suggestie gewekt dat deze geldt voor alle vormen van telecommunicatie: 'In het geval van nieuwe netwerken en/of telecommunicatiediensten moeten de aftapmogelijkheden niet alleen gecreëerd maar ook bekostigd worden door het bedrijfsleven; in totaal gaat het dan om circa 1% van de totale investeringskosten.'[70]

Beide beleidsvoornemens zijn vervolgens rechtstreeks verwerkt in de Telecommunicatiewet, eveneens met de argumentatie dat de kosten voor de overheid van aftappen almaar stijgen door technische ontwikkelingen, en dat als bijkomend voordeel van de kostenverdeling een prikkel wordt ingebouwd om zo voordelig mogelijk aftapbaarheid in te bouwen. 'Het beleid met betrekking tot de financiering van het aftappen van GSM wordt hiermee ook op andere telecommunicatiesystemen in Nederland van toepassing verklaard.'[71] De 1%-schatting voor de investeringskosten wordt herhaald door de minister,[72] waarbij zij zelfs aangeeft dat 1% een maximumschatting is, mits er in het beginstadium al rekening wordt gehouden met aftapbaarheid: 'Het aftapbaar maken van telecommunicatienetwerken en -diensten is bij installatie van nieuwe systemen relatief goedkoop. Meestal minder dan 1% van de investeringen. Het aftapbaar maken van bestaande systemen is zeer kostbaar.'[73] Deze schatting heeft een rol gespeeld bij de acceptatie van de kostenverdeling door het parlement, waartegen tijdens de behandeling de nodige weerstand werd geuit.[74] De kostenregeling in de Telecommunicatiewet werd aldus:

> **Artikel 13.6 TW (1998)**
>
> 1. De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn of worden gemaakt teneinde te kunnen voldoen aan de artikelen 13.1, 13.4, en 13.5 komen te hunner laste.
>
> 2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hebben aanspraak op vergoeding uit 's Rijks kas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een bijzondere last als bedoeld in artikel 13.2, eerste en tweede lid, onderscheidenlijk het verstrekken van informatie als bedoeld in artikel 13.4.
>
> 3. Bij ministeriële regeling worden regels gesteld met betrekking tot de vaststelling en vergoeding van de kosten, bedoeld in het tweede lid.

[67] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 10.
[68] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 10.
[69] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 14. Deze ruwe schatting was gebaseerd op een vertrouwelijk rapport van FEL/TNO uit maart 1994, nr. FEL-94-C104.
[70] *Kamerstukken II* 1995/96, 24 679, nr. 3, p. 5.
[71] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 126.
[72] 'In het bijzonder het aftapbaar maken van nieuwe netten en diensten is betrekkelijk eenvoudig en goedkoop (1% van de investeringskosten).' *Kamerstukken II* 1997/98, 25 533, nr. 82, p. 5. In vergelijkbare zin *Kamerstukken I* 1997/98, nr. 309b, p. 21, en *Handelingen I* 13 oktober 1998, 3-45, 3-63 en 3-67.
[73] *Kamerstukken I* 1997/98, 25 533, nr. 309d, p. 5. Zo ook *Handelingen II* 31 maart 1998, 67-5008.
[74] Zie het amendement-Leers, *Kamerstukken II* 1997/98, 25 533, nr. 23, dat werd verworpen, en uitspraken als 'ach, het is maar 1% van het investeringsbedrag' en 'bij 1% van de grote investeringen die het hier betreft, gaat het natuurlijk toch om grote bedragen.' *Handelingen II* 31 maart 1998, 67-5024 resp. 5015.

De ministeriële regeling uit het derde lid liet lang op zich wachten: pas in 2005 werd de Regeling kosten aftappen en gegevensverstrekking gelanceerd, waarin standaardbedragen zijn vastgesteld voor allerlei tapgerelateerde handelingen.[75]

2.6.2. Eenmalige tegemoetkoming

In 1996 werd voorzien voor bestaande netwerken en diensten een eenmalige tegemoetkoming in de kosten voorzien:

> **Beleidsvoornemen 7**
>
> Voor reeds operationele systemen betalen de Minister van Justitie en de Minister van Binnenlandse Zaken, overeenkomstig een door hen vast te stellen verdeelsleutel, eenmalige overgangsvergoedingen ten behoeve van het aftapbaar maken daarvan. Deze overgangsvergoedingen zijn f 2,9 miljoen groot. Dit bedrag is de helft van de totale investeringskosten om de reeds operationele systemen aftapbaar te maken. Daarmee komen dus ook f 2,9 miljoen ten laste van de netwerkbeheerders.

In de Telecommunicatiewet is deze eenmalige vergoeding niet opgenomen.[76] Uit openbare stukken valt niet op te maken of de eenmalige vergoeding is uitbetaald aan aanbieders (zie verder par. 5.1).

2.6.3. Kosten voor beveiliging

Naast investeringskosten voor aftapbaarheid, moeten aanbieders ook kosten maken om te kunnen voldoen aan de beveiligingsplichten die de geheimhouding van tapgerelateerde informatie moeten waarborgen (zie par. 2.7). Deze kosten zijn niet gekwantificeerd of uitgewerkt in de Telecommunicatiewet van 1998. Bij de concretisering van de beveiligingseis in een AMvB (zie par. 2.7) wordt wel een inschatting gemaakt van de kosten die aanbieders zullen moeten maken. De kosten voor het maken van een beveiligingsplan worden geraamd op gemiddeld € 2.200 per aanbieder, terwijl de kosten voor het jaarlijks actualiseren van dit plan geschat worden op gemiddeld € 220 per aanbieder. Het toezenden van de vereiste rapporten van verwijdering en vernietiging van gegevens worden lager ingeschat, op gemiddeld € 110 per aanbieder.[77] Het besluit gaat bij de totaalraming uit van 300 aanbieders.

2.7. Overige onderwerpen

2.7.1. Beveiliging en staatsgeheimen

Voor de Rijksdienst gelden voorschriften voor het beveiligen van staatsgeheimen. Gegevens over 'aftappen en informatieverstrekkingen die in het belang van de Staat geheim moeten worden gehouden, zijn formele staatsgeheimen en worden bij de overheid aan een beveiligingsregime onderworpen.'[78] Voor telecommunicatieaanbieders zou, aldus de beleidsnotitie uit 1996, een gelijkwaardige beveiliging moeten gelden, zowel personeel (door veiligheidsonderzoeken) als organisatorisch en fysiek:

> **Beleidsvoornemen 4**
>
> Netwerkbeheerders en dienstenleveranciers dienen een adequaat, bij wet opgedragen, beveiligingsregime in te richten.

Dit is vertaald in art. 13.5 van de Telecommunicatiewet:

> **Artikel 13.5 TW (1998)**
>
> 1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last als bedoeld in artikel 13.2 en informatieverstrekkingen als bedoeld in artikel 13.4 te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.

[75] Regeling van 30 maart 2005, *Stcrt.* 31 maart 2005, p. 16, inwerkingtreding 2 april 2005.
[76] 'Bedoelde tegemoetkomingen worden niet ingevolge het onderhavige wetsvoorstel verstrekt.' *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 127.
[77] Besluit beveiliging gegevens aftappen telecommunicatie, Stb. 2003, 472, p. 16.
[78] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 9.

> 2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging, bedoeld in het eerste lid.

De desbetreffende AMvB verscheen in 2003 als *Besluit beveiliging gegevens aftappen telecommunicatie*.[79] Dit besluit bevat een explicitering van beveiligingsmaatregelen, nader geconcretiseerd in een bijlage, die de vertrouwelijkheid en integriteit van gegevens rond aftappen en informatieleveringen beogen te garanderen. Voorts bevat het een verplichting tot het maken van een beveiligingsplan, een eis dat uitsluitend doorgelicht personeel met de uitvoering van tappen en informatielevering belast is,[80] een geheimhoudplicht, maatregelen te treffen bij het uitlekken van informatie, en een regeling bij uitbesteding van werkzaamheden.
De toelichting geeft aan dat de beveiligingsplicht van art. 13.5 in principe een zaak is voor aanbieders zelf om in te vullen. Nu er echter met de liberalisering meer aanbieders zijn, neemt de kans op inbreuken op de vertrouwelijkheid volgens de wetgever toe, en is het noodzakelijk om een minimumniveau aan beveiliging via een AMvB wettelijk te concretiseren.[81] Dit minimumniveau zou soms voor ivd's niet voldoende kunnen zijn; zij kunnen dan overleggen met aanbieders om aanvullende veiligheidsmaatregelen te treffen, maar zij kunnen deze niet wettelijk afdwingen.[82]
Hoewel de toelichting uit 2003 vermeldt dat het inmiddels noodzakelijk gevonden wordt om de beveiligingsplicht wettelijk te concretiseren, duurde het nog ruim anderhalf jaar voor het Besluit in werking trad, op 1 juni 2005. De inwerkingtreding zonderde art. 4 lid 1 van het Besluit uit, de verplichting om medewerking aan ivd-verzoeken alleen door personeel in vertrouwensfuncties te laten verrichten, vanwege de overbelasting die de grote hoeveelheid veiligheidsonderzoeken voor de AIVD met zich mee zou brengen.[83]

2.7.2. Geschillenbeslechting

Als sluitstuk van de regeling in hoofdstuk 13 kan worden gezien de bepaling die is opgenomen in art. 13.3, die een vorm van geschillenbeslechting bevat.

> **Artikel 13.3 TW (1998)**
>
> Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot het beslechten van geschillen tussen aanbieders en de bevoegde autoriteiten over de voorzieningen door middel van welke de door een tap te verkrijgen telecommunicatie door aanbieders wordt doorgegeven.

Opmerkelijk is dat deze regeling beperkt is tot geschillen over de voorzieningen voor het *doorgeven* van getapte telecommunicatie aan de autoriteiten. Voor alle andere onderwerpen waarover geschillen kunnen ontstaan, zoals over interpretatie van de technische aftapbaarheidseisen of van de beveiligingsplicht, staat alleen de gebruikelijke gang naar de rechter open voor aanbieders of behoeftestellers,[84] wat een ingrijpender – en vaak ook langduriger – stap is dan een alternatieve vorm van geschillenbeslechting in te roepen.

2.7.3. Toezichthouders en overleg

De algemene toezichthouder voor de Telecommunicatiewet is de OPTA.[85] Voor hoofdstuk 13 werd echter een specifieke toezichthouder aangewezen op basis van art. 15.1 lid 1 onder e, de afdeling Veiligheid en Nummering van de Directie Informatie-infrastructuur van de Hoofddirectie Telecommunicatie en Post.[86] Het toezicht werd op 1 september 2002 overgeheveld naar de divisie Telecom van de Inspectie Verkeer en Waterstaat, waarmee 'een verdere scheiding tussen

[79] Besluit van 28 oktober 2003 (Besluit beveiliging gegevens aftappen telecommunicatie), Stb. 2003, 472.
[80] Voor medewerking met ivd's betekent dit dat personen een vertrouwensfunctie als bedoeld in de Wet veiligheidsonderzoeken dienen uit te oefenen; voor medewerking met justitie gaat het om personen van wie een verklaring omtrent het gedrag is overgelegd.
[81] Besluit beveiliging gegevens aftappen telecommunicatie, Stb. 2003, 472, p. 7-8.
[82] Besluit beveiliging gegevens aftappen telecommunicatie, Stb. 2003, 472, p. 8.
[83] Besluit van 8 maart 2005, Stb. 2005, 141.
[84] Bij klachten van behoeftestellers treedt de inspecteur van het Agentschap Telecom bemiddelend op, aldus de nieuwsbrief *Aftapverplichting voor aanbieders van openbare telecommunicatie diensten en –netwerken*, 23 maart 2004, <http://www.at-ez.nl/informatie/publicaties/nieuwsbrieven/nb_0404_hh.html>. 'Het doel van de inspecteur is hierbij vooral om de gewenste tapinformatie onverwijld bij de behoeftesteller te krijgen.'
[85] Art. 15.1 lid 3 TW jo. Wet Onafhankelijke post- en telecommunicatieautoriteit.
[86] Besluit aanwijzing toezichthouders Telecommunicatiewet, *Stcrt.* 1998, nr. 230, p. 9.

beleid en handhaving bewerkstelligd' werd.[87] Bij de overdracht van taken op het gebied van telecommunicatie van V&W naar EZ werd de divisie Telecom hernoemd in het agentschap Telecom (AT) van het Ministerie van Economische Zaken, de huidige toezichthouder voor hoofdstuk 13 TW.[88] Voor de onderdelen van hoofdstuk 13 die persoonsgegevens betreffen, zoals art. 13.2a en 13.4, kan ook het College Bescherming Persoonsgegevens (CBP) toezicht houden.

In aanvulling op de regeling van geschillenbeslechting en het toezicht, is ook voorzien in een geformaliseerd regulier overleg tussen aanbieders en behoeftestellers. Dit overleg hoorde thuis in het permanente Overlegorgaan Post en Telecommunicatie (OPT), maar omdat er te veel aftaponderwerpen waren voor het algemene overleg binnen dit orgaan, is per 1 januari 1999 een Deelorgaan aftappen (DAF) ondergebracht bij het OPT. Hierin zal 'overlegd worden over de uitvoering van de regelgeving inzake het bevoegd aftappen en zullen afspraken worden gemaakt met de bevoegde autoriteiten. Het deelorgaan aftappen zal op het gebied van aftappen als platform fungeren voor de uitwisseling van informatie en afstemming tussen de overheid en de aanbieders van telecommunicatienetwerken en telecommunicatiediensten.'[89] In het Instellingsbesluit werden limitatief de organisaties (hoofdzakelijk telecomaanbieders en brancheorganisaties) aangewezen die zich in DAF kunnen laten vertegenwoordigen. Tot medio 2002 vond regelmatig overleg plaats binnen DAF, maar omdat langzamerhand de belangrijkste onderdelen van de wet waren ingevuld, werd in april 2004 besloten DAF op te heffen en voortaan de formele besluitvorming weer binnen OPT te doen plaatsvinden. Aangezien er daarnaast behoefte was om informeel te overleggen, werd tegelijk een Coördinatie Commissie Aftappen (CCA) ingesteld. Hierin kunnen discussies worden gevoerd voorafgaand aan besluitvorming binnen OPT. Naast DAF/CCA vindt ook overleg plaats op operationeel terrein tussen Openbaar Ministerie en aanbieders in het zogeheten TACO-overleg (Telecommunicatie Aftap Coördinatie Overleg).

2.8. Afsluiting

In een notendop heeft Kamerlid Kamp het aftapbaarheidsbeleid verwoord: 'De oorspronkelijke vorm van telefonie is afluisterbaar. Een alternatief moet dat ook zijn. Wij zijn van mening dat het afluisterbaar zijn een noodzakelijk, onlosmakelijk onderdeel is van de verschijningsvorm telefonie in ons land.'[90] Dit 'onlosmakelijke onderdeel' is aldus op simpele wijze getransponeerd van de oude PTT-telefoniewereld naar de nieuwe vormen van telecommunicatie. Het uitgangspunt 'wat off-line geldt, moet ook on-line gelden'[91] komt hier in optima forma tot uitdrukking.
Het is de vraag of het zo simpel is: de techniek heeft zoveel eigen aspecten en dynamiek dat het vertalen van een eigenschap van de traditionele vaste telefonie naar het hele brede spectrum van moderne telecommunicatie de nodige problemen oplevert. Sinds eind jaren negentig is de telecommunicatiemarkt in korte tijd in zo goed als alle denkbare opzichten dramatisch veranderd. De technische ontwikkelingen hebben zich in de afgelopen vijf tot tien jaar in versneld tempo voortgezet. Als gevolg van de liberalisering is de marktdynamiek volledig veranderd. Er zijn nieuwe netwerken bijgekomen, zoals draadloze toegangsnetwerken, en een explosie aan diensten is zichtbaar, mede door toenemende convergentie van verschillende netwerken, basisdiensten en toegevoegdewaardediensten. Deze veranderingen in techniek en markt zetten het aftapbaarheidsbeleid onder druk. Hoe wordt in dat licht momenteel, ruim zes jaar na inwerkingtreding van de Telecommunicatiewet, aangekeken tegen het beleid en de wetgeving uit de jaren negentig? In de volgende hoofdstukken beantwoorden we deze vraag voor de verschillende onderdelen van het aftapbaarheidsbeleid.

[87] Wijziging Besluit aanwijzing toezichthouders Telecommunicatiewet, *Stcrt.* 8 juli 2002, nr. 127, p. 12.
[88] Wijziging Besluit aanwijzing toezichthouders Telecommunicatiewet, *Stcrt.* 11 december 2003, nr. 240, p. 19. Zie ook <http://www.agentschap-telecom.nl/>.
[89] Instellingsbesluit deelorgaan aftappen van 21 mei 1999, *Stcrt.* 1999, nr. 108, p. 8, inwerkingtreding met terugwerkende kracht tot 1 januari 1999.
[90] *Handelingen II* 25 oktober 1995, 17-1123.
[91] Zoals gehanteerd in de Nota wetgeving voor de elektronische snelweg, *Kamerstukken II* 1997/98, 25 880, nrs. 1-2.

Deel II. Heden: bevindingen uit de vraaggesprekken

3. Uitgangspunt: "Openbare telecommunicatie is aftapbaar"

3.1. Technische aftapbaarheid

Mate waarin aan het uitgangspunt wordt voldaan
Behoeftestellers en aanbieders verschillen in hun inschatting van de mate waarin aan het uitgangspunt wordt voldaan.

De behoeftestellers geven aan dat de aanbieders zich slecht aan de wet houden en dat belangrijke delen van het telecommunicatieverkeer feitelijk niet aftapbaar zijn. Eigenlijk geldt voor alle vormen van telecommunicatie dat er overal gaten zitten in de aftapbaarheid'. Openbare diensten en netwerken zijn vaak niet aftapbaar op het moment dat ze worden geïntroduceerd op de markt. Bij de meeste daarvan wordt dat in de loop van de tijd verholpen, maar er zijn er ook waar het ook na lange tijd niet opgelost was. Zeker bij specifieke vormen van diensten en bij het gebruik van toegevoegdewaardediensten blijven er langdurig problemen. Bij de behoeftestellers viel in deze context ook de term 'welwillende tegenwerking', met name waar het voldoen aan de technische voorzieningen betreft.

Het oordeel van de aanbieders luidt anders. Daar valt te beluisteren dat nagenoeg alle telefoniediensten goed aftapbaar zijn. Bij nieuwe diensten komt er soms wel vertraging voor, maar het is uiteindelijk maar een fractie van het verkeer waar aftappen problematisch is. Bij Internetdiensten ligt dat volgens de aanbieders mogelijk wat anders: Internettoegangsdiensten en e-mail zijn in elk geval bij de grotere ISP's aftapbaar, maar bij kleine en middelgrote ISP's deels wel en deels niet aftapbaar. Een relevant punt is daar dat Internetaanbieders van oudsher een wat andere cultuur kennen dan de traditionele telecommunicatieaanbieders. De "spontane naleving"[92] bij Internet is laag, ook al is de ontheffing voor Internetaanbieders reeds in 2001 afgelopen. Via de brancheverenigingen NLIP legt de toezichthouder AT contact met Internetaanbieders, waardoor de aftapplicht meer gaat leven bij de kleine aanbieders. De voorziening in de vorm van een verplaatsbare tapkast die diverse aanbieders hebben getroffen binnen het Nationale Beheerorganisatie Internet Providers (NBIP), waarbij inmiddels zo'n 25 aanbieders zijn aangesloten, wordt als een goed systeem gezien om Internetaanbieders aan de tapplicht te laten voldoen zonder dat zij zelf alle benodigde kosten individueel hoeven te maken.

De beschikbaarheid van de benodigde aftapspecificaties (normen)
Om succesvol een afgetapt signaal van operator over te dragen naar behoeftesteller zijn er technische specificaties ofwel normen nodig. De belangrijkste in Nederland gebruikte normen zijn ETSI-NL (voor telefonie) en TIIT (voor Internet) (zie par. 2.4.4). Specifieke technieken en diensten (denk aan bijvoorbeeld GPRS, UMTS, WiFi, VoIP) vragen echter om aanvullingen op normen of nieuwe normen.

Behoeftestellers stellen dat het grote probleem is dat operators lang niet altijd tijdig aan hen melden wanneer ze een nieuwe dienst aanbieden. Dat gebeurt soms enkele dagen van tevoren, terwijl het noodzakelijk is om deze informatie veel langer vooraf te ontvangen zodat de technische specificaties voor het aftappen kunnen worden vastgesteld. Daardoor zijn nieuwe diensten niet aftapbaar, ook wanneer het om breed geïntroduceerde massadiensten gaat. Diverse aanbieders stellen echter dat zij bij bepaalde nieuwe technieken in een vroeg stadium de overheid hadden verzocht om aftapspecificaties te ontwikkelen, maar dat daarop dan niet gereageerd werd. Een voorbeeld dat een aanbieder gaf, betreft de ontwikkeling van een VoIP-dienst waarbij twee jaar geleden aan de overheid werd gevraagd om duidelijke regels voor de aftapbaarheid hiervan, waar tot nu toe geen reactie op is gekomen.

[92] Het naleven van de wet zonder daar door de toezichthouder apart toe aangemaand te worden.

Behoeftestellers geven aan dat het initiatief voor de aankondiging van een nieuwe dienst bij de operators ligt, en dat daarbij ook specificaties van de gebruikte techniek nodig zijn. Alleen op basis daarvan kan DGTP de specificaties vaststellen. Wij kunnen daar echter als onderzoekers tegenover stellen dat een marktintroductie van een belangrijk aantal diensten waar het hier over gaat, ook zonder een kennisgeving van de operator was te voorzien. Nadat bedrijven in het jaar 2000 grote sommen geld hadden uitgegeven voor een UMTS-licentie, was het evident dat die techniek en de daarbij horende netwerken en diensten na enige tijd op de markt zouden komen. Het betreft hier een Europese norm, voortgebracht door ETSI/3GPP, die voor alle geïnteresseerden vrij beschikbaar is. Een vergelijkbaar verhaal geldt voor de introductie van bijvoorbeeld GPRS. In dergelijke gevallen zou de overheid zelf meer initiatief kunnen nemen. De meeste aanbieders geven ook aan een meer pro-actieve rol van de overheid op prijs te stellen; DGTP zou daarbij een actievere rol kunnen vervullen. De haalbaarheid van een pro-actievere overheidsrol bij de ontwikkeling van specificaties hangt echter mede af van de technische kennis die de overheid in huis heeft, en die wordt door de aanbieders niet hoog ingeschat.

Veel diensten zijn op het moment dat zij worden geïntroduceerd nog in een testfase, waarbij ook de aftapbaarheid vaak nog moeten worden uitgetest. In die fase zijn vaak veel bedrijfsinterne processen nog niet goed geregeld, zoals facturering. Zonder vroegtijdige technische aftapspecificaties is het daarom voor aanbieders vaak onmogelijk om te zorgen dat de dienst al bij introductie aftapbaar is. Overigens worden de specificaties, wanneer ze wel beschikbaar zijn, door sommige aanbieders ook onvoldoende gedetailleerd gevonden: er blijven nog de nodige interpretatievragen over die op de werkvloer opgelost moeten worden.
De behoeftestellers stellen zich op het standpunt dat, wat er ook zij van technische complicaties of onderlinge afstemming, het hele proces van ontwikkelen en testen van aftapbaarheid moet plaatsvinden vóórdat een netwerk of dienst op de markt wordt gebracht. Dat staat nu eenmaal zo in de wet, en daaraan hebben aanbieders zich te houden. De aanbieders ervaren het vaak als onmogelijk om zich zo strikt aan de wet te houden, omdat dit de uitrol van nieuwe diensten of netwerken enorm zou vertragen (terwijl de ontwikkelfase toch al vaak langer duurt vanwege de noodzaak aan aftapbaarheid aandacht te besteden), en bovendien het testen of alles werkt toch in de praktijk moet gebeuren en dus juist niet alleen maar voor introductie op de markt kan plaatsvinden.

Aftapspecificaties (normen) in een internationale context
De implementatie van bepaalde aftapspecificaties brengt vanzelfsprekend kosten met zich mee. Daarbij is het van bijzonder belang hoe groot de markt voor producten conform die specificaties is. In Nederland worden specifieke Nederlandse normen gebruikt, te weten ETSI-NL en TIIT. Daarbij moeten we direct opmerken dat het niet zo is dat alleen Nederland afwijkt in het gebruik van nationale normen. Dat komt vaker voor, en bovendien is er voor Internetverkeer nog geen internationale breed gedragen norm. Hier speelt ook een rol dat Nederland relatief gezien voorop loopt met het aftappen, zeker op Internetgebied.
Op een grote, internationale markt ontstaat er snel mededinging en zal de benodigde aftapapparatuur een aantrekkelijk prijsniveau krijgen. Als er sprake is van een heel kleine markt (bijvoorbeeld bij een afwijkende, nationale standaard) ligt dat heel anders. Apparatuur kan, mede door gebrek aak keuze, zeer kostbaar zijn. Sommige operators geven aan dat de toeleveranciers van hun netwerken het simpelweg weigeren om specifieke nationale aftapspecificaties te implementeren, of dat alleen doen tegen onredelijk hoge vergoedingen. Zij vinden de Nederlandse markt simpelweg te klein en te weinig interessant. Het probleem wordt versterkt doordat operators om diverse redenen min of meer verplicht zijn hun netwerken van nieuwe softwareversies te voorzien, de zogenoemde *releases*. Elke keer kan het goed (blijven) werken van de aftapvoorzieningen weer een probleem zijn.
Niet alleen bij toeleveranciers speelt dit punt; de dienstenontwikkeling van grote, internationale netwerkoperators vindt ook steeds vaker op één enkele locatie plaats. Vervolgens wordt de desbetreffende dienst uitgerold in alle landen. Daarbij wordt vaak maar in beperkte mate rekening gehouden met de specifieke (aftap)behoeften in één bepaald land. Ook in dat opzicht kunnen afwijkende nationale normen dus problematisch zijn.
We moeten bij de operators echter ook een zekere dubbelheid vaststellen waar het de aftapspecificaties betreft. Enerzijds beklagen zij zich om de specifieke NL-specificaties bij

telefonie en bij Internettappen, welke zouden leiden tot onnodige kosten, maar anderzijds geven zij aan dat de overheid actiever moet zijn met het opstellen van specificaties, omdat anders niet aan de verplichting kan worden voldaan. Dit is een klassiek dilemma van timing: wanneer zijn de gevolgen van te vroeg zijn en die van te laat zijn goed met elkaar in balans?

Specifieke problemen bij kleinere aanbieders
Een wezenlijk aandachtspunt is dat de markt sinds 1998 enorm is veranderd: waar vroeger de aanbieders van telecommunicatie op de vingers van één hand waren te tellen, zijn er nu alleen al 350 aanbieders van Internetdiensten actief. Daar zijn ook heel veel kleine aanbieders bij, en die hebben soms geen idee hoe ze met aftapbaarheid om moeten gaan. Ook registreren niet alle kleinere aanbieders zich bij OPTA, zeker waar het dienstenleveranciers betreft. Wellicht dat de registratiekosten daar een rol bij spelen. Eén kleine aanbieder merkte op dat hij niet alle wetten en specificaties kon uitpluizen; daardoor "weet je pas dat je niet voldoet aan de verplichting als je een boete krijgt". Deze uitspraak komt niet overeen met de werkelijkheid van handhaving (waarbij aanbieders vaak wel enige tijd wordt gegund om alsnog te voldoen aan de wet), maar tekent wel het beeld dat bij kleine aanbieders bestaat van ingewikkelde wetgeving die ergens als een zwaard van Damocles in de ruimte hangt.

Benodigde voorzieningen bij de overheid
Om succesvol af te tappen moet ook de behoeftesteller voorzieningen installeren zodat het signaal volgens de afgesproken specificaties kan worden overgedragen. Operators geven aan dat deze voorzieningen in sommige gevallen niet goed zouden werken of ondergedimensioneerd zijn (ze lopen 'over' bij een zware gebruiker); soms viel zelfs te beluisteren dat de operators vermoedden dat er door de regelgever wel normen waren opgelegd maar dat de behoeftestellers zelf helemaal niet hadden geïnvesteerd in de benodigde apparatuur om de binnenkomende gegevens volgens die normen te ontvangen. De behoeftestellers geven echter juist aan dat zij vaak over de benodigde, dure 'ontvangstapparatuur' beschikken, maar dat deze weg staat te roesten omdat de operators hun plicht niet nakomen en de benodigde 'zendapparatuur' niet installeren.

Conclusies over de huidige mate van aftapbaarheid.
Concluderend kan worden gesteld dat het overgrote deel van de openbare telecommunicatie grotendeels aftapbaar lijkt te zijn (zie Kader 3.1), hoewel de behoeftestellers en de aanbieders van mening verschillen over hoe groot of hoe belangrijk het niet-aftapbare deel is. Dit niet-aftapbare deel betreft voornamelijk specifieke varianten op diensten, en het oordeel over de omvang van deze diensten en het ' belang' ervan in de aftapcontext verschillen sterk. Niet-aftapbare delen worden onder meer veroorzaakt door een gebrek aan tijdige aftapspecificaties. Behoeftestellers en aanbieders verwijten elkaar de oorzaak te zijn voor dat probleem. Het hanteren van een afwijkende, Nederlandse norm heeft wel belangrijke kostenconsequenties, maar lijkt ons geen verklaring te zijn voor het nog bestaan van niet-aftapbare netwerken en diensten.
Al met al lijkt de wettelijke verplichting van art. 13.1 TW wel in behoorlijke mate effect te sorteren, al wordt de eis van volledige aftapbaarheid in deze bepaling zeker niet waargemaakt. Het belangrijkste knelpunt in de verplichting is de clausule 'vanaf het moment van introductie' die impliciet[93] in de wet is opgenomen: de meeste nieuwe telecommunicatie is pas na enig verloop van tijd, werkendeweg, aftapbaar.

- Vaste telefoniediensten en hun onderliggende netwerken: zo goed als volledig aftapbaar, behoudens bepaalde specifieke diensten en dienstvarianten.
- Mobiele telefoniediensten en hun onderliggende netwerken: zo goed als volledig aftapbaar, vooral bij de oudere generaties mobiele telefonie, behoudens bepaalde specifieke diensten en dienstvarianten.
- Internettoegangsdiensten en e-mail: grotere ISP's volledig aftapbaar, behoudens bepaalde specifieke diensten en dienstvarianten; kleine en middelgrote ISP's deels aftapbaar (bijv. via NBIP) en deels niet aftapbaar.

[93] De clausule staat – tussen haakjes (!) – in het beleidsuitgangspunt uit 1996; in art. 13.1 komt zij impliciet tot uitdrukking in de woorden 'stellen (...) uitsluitend beschikbaar aan gebruikers'.

Kader 3.1: Overzicht van de huidige mate van aftapbaarheid van Nederlandse netwerken en diensten[94]

3.2. Openbaarheid

Wat is precies openbaar?

Een openbaar telecommunicatienetwerk is volgens de definitie in de TW een netwerk 'dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden', terwijl een openbare telecommunicatiedienst een 'voor het publiek beschikbare dienst' is (art. 1.1 onder ee en ff TW). Kenmerkend voor openbaarheid is dus dat een telecommunicatiedienst voor het publiek beschikbaar is, dat wil zeggen dat er sprake moet zijn van een openbaar aanbod en van beschikbaarheid voor iedereen tegen in het openbaar aanbod vermelde voorwaarden; daaronder vallen niet besloten gebruikersgroepen (zie par. 2.4.2).

Een besloten groep kan echter wel in zekere mate ruim zijn – de minister gaf in de kamerbehandeling van de TW aan dat niet-openbare netwerken of diensten aftapbaar gemaakt kunnen worden, via art. 13.7 TW, 'indien, ondanks het feit dat het netwerk of dienst *niet openbaar* is, de kring van gebruikers *zodanig ruim* is dat aftapbaarhied [sic] toch noodzzakelijk [sic] is in verband met genoemde belangen' van staatsveiligheid en opsporing (onze cursivering).[95] Dat is kennelijk minder ruim dan de situatie waarin 'closed user groups (...) een dergelijke omvang aannemen dat het eigenlijk meer abonnees zijn geworden. Het MKB Nederland denkt nu na over een closed user group met alle winkels in Nederland en dan kan toch moeilijk worden volgehouden dat dit nog een gesloten netwerk is?'[96] Waar de grens ligt tussen een zo ruime groep dat er sprake is van een openbaar aanbod en een groep die zo ruim is dat deze afgetapt moet kunnen worden maar die toch besloten is, is niet te vinden in de parlementaire geschiedenis van de Telecommunicatiewet. De vantoepassingverklaring van de vroegere interpretatie van het begrip 'gesloten gebruikersgroep' onder de Wtv op de 'besloten groep' van de TW (zie par. 2.4.2) is daarom het enige aanknopingspunt. Hieronder werden verstaan ondernemingen die deel uitmaken van dezelfde economische eenheid, en groepen waarvan de leden een duurzame relatie onderhouden van economische of professionele aard, zoals branchegenoten of relatienetwerken van ondernemingen.[97] Nog los van de vraag of deze transponering van het Wtv-begrip, dat in het kader van liberalisering werd gehanteerd, juist is,[98] biedt ook deze aanduiding nog niet veel houvast. In de literatuur wordt dan ook geconcludeerd dat 'de invulling van het begrip openbaarheid niet alleen thans onduidelijk is', en bovendien dat 'naar verwachting de onduidelijkheden eerder groter dan kleiner zullen worden.'[99]

Niettemin moet wel worden opgemerkt dat de wetgever onlangs meer houvast heeft geboden. Bij de vergunningverlening voor Public Access Mobile Radio-frequentieruimte wordt de volgende toelichting gegeven: 'een besloten gebruikersgroep bestaat uit gebruikers van elektronische communicatiediensten die onderling een duurzame professionele relatie hebben en daardoor binnen de groep een communicatiebehoefte hebben die voortvloeit uit het gemeenschappelijke belang dat aan deze duurzame relatie ten grondslag ligt. De duurzame professionele relatie omvat meer dan alleen het gezamenlijk afnemen van elektronische communicatiediensten en de besloten gebruikersgroep is niet uitsluitend opgezet om elektronische communicatiediensten af te nemen.'[100]

Desondanks blijkt er in de praktijk nog de nodige verwarring en onzekerheid te bestaan over de interpretatie van het begrip 'openbaarheid'. Enkele voorbeelden die in de vraaggesprekken zowel bij aanbieders als bij behoeftestellers en derden werden genoemd met betrekking tot *netwerken* zijn de volgende.

- De definitie van een openbaar netwerk als een netwerk met een openbare dienst suggereert voor sommigen dat ook netwerken in bijvoorbeeld bejaardenhuizen, scholen of van woningbouwverenigingen onder dit begrip vallen, als zij Internettoegang aan hun

[94] Over de aftapbaarheid van vanuit het buitenland geleverde diensten, zie par. 3.4.
[95] *Kamerstukken II* 1997/98, 25 533, nr. 5. p. 133-134.
[96] *Kamerstukken II*1995/96, 24 679, nr. 3, p. 6.
[97] Hein Dries, Serge Gijrath & Paul Knol, *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, ITeR-deel 60, Den Haag: Sdu 2003, p. 38, gebaseerd op de genoemde Bekendmakingen van de minister van V&W inzake begrip 'derden' bij spraakverkeer vaste verbindingen (*Stcrt.* 1994, nr. 103, p. 14) en inzake Spraakverkeer over vaste verbindingen door middel van 'dial-in' of 'dial-out' (*Stcrt.* 1995, nr. 84, p. 9-10).
[98] Dries c.s. hebben 'gerede twijfel of het zonder meer toepassen van de historische beschrijving van de "besloten gebruikersgroep" zinvol is'. *Ibid*., p. 39,
[99] *Ibid.*, p. 26. Zie p. 24-26 en daar aangehaalde literatuur van Van Eijk en Dommering ter onderbouwing van deze conclusie.
[100] <http://www.agentschap-telecom.nl/pamr/pamr_hme.html>.

gebruikersgroepen bieden. Hetzelfde geldt voor bijvoorbeeld openbare bibliotheken die toegang bieden tot het Internet op een aantal computers: hebben zij daardoor een openbaar telecommunicatienetwerk?
- Locale WiFi-netwerken; als 'voor het publiek beschikbaar' betekent voor 'eenieder die toegang wil krijgen', zou men deze als openbaar kunnen beschouwen, omdat in beginsel iedereen zich in de buurt van een lokaal WiFi-netwerk kan begeven en dan van het netwerk gebruik kan maken om het Internet op te gaan; betekent het echter 'voor iedereen in Nederland toegankelijk', dan is een lokaal netwerk niet openbaar; de vraag of een geografische beperking leidt tot openbaarheid is tot nu toe niet eenduidig beantwoord.[101]
- Locale glasvezelnetwerken; deze werden in vraaggesprekken, vanwege dezelfde onduidelijkheid over geografische beperking, door sommigen als besloten aangemerkt omdat alleen de locale bewoners er toegang toe hebben; zij achtten dat problematisch wanneer deze netwerken een grote omvang krijgen en dan niet aftapbaarheidsplichtig zouden zijn.

Ook op het gebied van *diensten*, en vooral bij mengvormen tussen netwerken en diensten met verschillende partijen, bestaat bij de geïnterviewde partijen onduidelijkheid over de reikwijdte van het begrip openbaarheid. Voorbeelden die herhaaldelijk in de interviews zijn genoemd, betreffen:
- VPN-diensten, waarbij een telecomaanbieder netwerkcapaciteit aanbiedt aan besloten gebruikersgroepen, zoals bedrijfsnetwerken, waarbij eindgebruikers over de huurlijn zelf aan weerszijden encryptie gebruiken; nu heeft de minister bij de beleidsvorming in 1996 wel aangegeven dat VPN-diensten als openbaar moeten kunnen worden aangewezen,[102] maar nu huurlijnen wel en VPN niet in art. 2 van de Regeling aftappen zijn aangewezen als openbare netwerken of diensten waarvoor nadere technische eisen zijn gesteld, rijst de vraag of VPN-diensten zonder specifieke aanwijzing wel als openbaar kunnen worden beschouwd; een vergelijkbare problematiek betreft e-maildiensten waarbij de afnemers zelf de aliassen en wachtwoorden tot de e-mail beheren;
- collocatie (ook soms gespeld als colocatie). Dit is een systematiek waarbij derden (eindgebruikers, bedrijven, enzovoorts) de gelegenheid hebben om apparatuur zoals web- en mailservers te plaatsen op een locatie van de dienstaanbieder. Dit biedt veel voordelen: er is een directe en snelle verbinding met het netwerk en belangrijke voorzieningen als noodstroom en koeling zijn allemaal voorhanden. Tijdens de vraaggesprekken bleek dat er veel onduidelijkheid heerst in hoeverre collocatiediensten geraakt worden door de aftapverplichting;
- aanbieders van faciliteiten voor gesloten gebruikersgroepen op het Internet of bij UMTS, zoals chatgroepen, blogs of thuispagina's die slechts na registratie voor leden van een bepaalde groep beschikbaar zijn; als dit een gebruikersgroep is die een duurzame relatie onderhoudt van economische of professionele aard, is er geen sprake van een openbare dienst, maar waar ligt de grens van een dergelijke groep?

Deze voorbeelden geven aan dat er een behoorlijk grijs gebied ervaren wordt tussen openbare en besloten telecommunicatie. Wellicht is dit grijze gebied voor specialisten in het telecommunicatierecht niet zo groot, maar voor partijen die er in de praktijk mee te maken hebben is het kennelijk moeilijk om de criteria voor openbaarheid toe te passen. Er is daarom dringend behoefte aan meer duidelijkheid over de afbakening van dit begrip.

Wie bepaalt wat openbaar is?

Wanneer bepaald moet worden of een aanbieder een openbaar of besloten netwerk of dienst levert, is een complicatie dat er twee toezichthouders zijn, OPTA en AT, met mogelijk verschillende interpretaties van dit begrip. De interpretatie van de OPTA is leidend: zij bepaalt wat een openbare en dus registratieplichtige aanbieder is. Dat gebeurt echter primair vanuit de visie op het toezicht houden op de elektronischecommunicatiemarkt, met een marktordeningsperspectief. Voor de toepasselijkheid van hoofdstuk 13 is echter ook de Regeling aftappen openbare telecommunicatienetwerken en -diensten relevant, die in artikel 2 een aantal soorten openbare netwerken en diensten met name aanwijst als vallend onder de aftapbaarheidsplicht. OPTA lijkt echter deze Regeling niet te gebruiken bij het bepalen van de

[101] Dries c.s. stellen dat een 'aanbod voor een geografisch beperkt gebied (...) niet per definitie tot niet-openbaarheid [lijkt] te leiden', *ibid.*, p. 40, daarmee suggererend dat het in bepaalde gevallen wel tot niet-openbaarheid leidt. Volgens Nico van Eijk (persoonlijke mededeling, 5 juli 2005) is geografisch gebied echter geen relevant criterium.

[102] 'Indien over een netwerk ook diensten worden afgewikkeld van niet-openbare aard (o.m. Gesloten Gebruikersgroepen, Virtual Private Networks en huurlijnen) willen wij deze diensten specifiek als openbaar kunnen aanwijzen indien daartoe op grond van de veiligheid van de Staat en/of de handhaving van de rechtsorde aanleiding bestaat.' *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 8.

'openbare' markt, zodat aanbieders van netwerken of diensten die in de Regeling worden genoemd niet noodzakelijkerwijs als 'openbaar' worden beschouwd. Daardoor kan een discrepantie ontstaan tussen wat AT beschouwt als een 'openbare' en dus aftapplichtige aanbieder op grond van de Regeling en wat OPTA aanwijst als 'openbare' en dus registratieplichtige aanbieder.[103] In de praktijk heeft dit overigens (nog) niet tot problemen geleid, maar theoretisch is het bepaald geen elegante constructie.

Besloten netwerken

Het vraagstuk van besloten netwerken is een belangrijk aandachtspunt. Deze netwerken vallen niet onder de Telecommunicatiewet en niet onder de aftapbaarheidsplicht. Art. 13.7 TW bevat weliswaar een mogelijkheid om ook besloten netwerken te kunnen aanwijzen om aftapbaar te maken (op kosten van de overheid), maar deze bepaling is niet in werking getreden (zie par. 2.4.2).

Omdat besloten netwerken enorm groot kunnen zijn, worden vraagtekens geplaatst bij de uitsluiting van de aftapbaarheidseis. Met name werden netwerken van multinationale ondernemingen en het netwerk van de universiteiten en HBO's herhaaldelijk genoemd als voorbeeld. De consequentie van het niet-aftapbaar hoeven zijn van deze netwerken is dat de netwerkaanbieder die toegang tot het openbare telecommunicatienetwerk verzorgt, verantwoordelijk is voor het tappen, waarbij dan al het verkeer van en naar het besloten netwerk wordt getapt, ook als slechts één interne gebruiker moet worden afgetapt. Dit is ondoelmatig en ook vanuit privacyoogpunt disproportioneel.

Men vergelijke daarbij ook de benadering die de wetgever nu hanteert in het hernieuwde wetsvoorstel Computercriminaliteit II, waarin het Cybercrime-verdrag wordt geïmplementeerd door onder andere ook besloten telecommunicatie te kunnen aftappen. Volgens dit voorstel kan op basis van art. 126m en 126t Sv telecommunicatie worden getapt 'die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst', en de definitie van zo'n aanbieder, in voorgesteld art. 126la, omvat zowel openbare als besloten telecommunicatie.[104] Daarmee nemen de aftapbepalingen in het Wetboek van Strafvordering afstand van de aftapbaarheidsbepalingen uit hoofdstuk 13 TW. In de praktijk zal menig beslotennetwerkbeheerder ook vaak in staat zijn mee te werken, aangezien veel (grote) bedrijven en instellingen tegenwoordig een beleid hebben voor controle van Internet- en e-mailverkeer van werknemers.

Dat betekent niet dat eventuele uitbreiding van de aftapbaarheidsverplichting naar besloten netwerken zonder meer wenselijk is. Het CBP noemt art. 13.7 TW juist één van de belangrijkste knelpunten in het beleid en pleit voor afschaffing hiervan. En ook vanuit het perspectief van OPTA rijzen hier vraagtekens: de Telecommunicatiewet beoogt openbare elektronische communicatienetwerken en -diensten te regelen, met definities hiervan in art. 1.1 TW, en het wekt bevreemding als er kennelijk netwerken of diensten zijn die niet openbaar zijn volgens art. 1.1 maar wel 'feitelijk openstaa[n] voor derden' volgens art. 13.7. Daarom lijkt de bepaling van art. 13.7 om de aftapbaarheidsverplichting in concrete gevallen uit te kunnen breiden tot besloten netwerken of diensten een vreemde eend in de TW-bijt.

Niettemin geven de behoeftestellers aan dat het niet-aftapbaar zijn van besloten netwerken een knelpunt is en dat zij inwerkingtreding van art. 13.7 wensen. Aan de andere kant wordt door andere geïnterviewden opgemerkt dat er kennelijk geen behoefte is aan inwerkingtreding, omdat hiertoe nog geen concrete stappen zijn ondernomen. Hierbij moet worden opgemerkt dat de investeringskosten bij het gebruik van art 13.7 voor rekening van de overheid komen, en dat de technische inrichting en afstemming een complexe aangelegenheid is, wat gebruikmaking van art. 13.7 minder aantrekkelijk maakt.

Conclusies over openbaarheid

Op basis van de bevindingen kunnen we stellen dat bij het vraagstuk van openbaarheid duidelijk naar voren komt dat de opname van aftapbaarheidsbepalingen in de Telecommunicatiewet botst met het karakter van deze wet. De Telecommunicatiewet gaat over openbare telecommunicatie, met het doel de markt te ordenen; verplichtingen voor besloten telecommunicatie, zoals in 13.7

[103] Daarnaast werd in vraaggesprekken ook opgemerkt dat de lijst van openbare aanbieders die OPTA hanteert, niet volledig is, omdat die lijst in eerste instantie zou uitgaan van wie zich geregistreerd heeft en niet van wat zich feitelijk op de markt voordoet.

[104] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 25-26. Of dit een juiste interpretatie is van de eisen die het Cybercrime-verdrag stelt, valt buiten het bestek van dit onderzoek.

TW, passen daar niet in. Dit spanningsveld blijkt ook in het toenemende grijze gebied van netwerken en diensten waarvan niet duidelijk is of ze openbaar zijn of niet; vanuit het oogpunt van de behoefte aan aftapbaarheid wordt dit grijze gebied anders geïnterpreteerd dan vanuit het oogpunt van marktordening. Er is dringende behoefte aan meer duidelijkheid over de aanwijzing van wat aftapbaar moet zijn in de zin van hoofdstuk 13 TW. Dit geldt enerzijds besloten netwerken of diensten die dermate groot zijn dat een substantieel deel van de telecommunicatie in Nederland via deze plaatsvindt (waarvan sommigen zich afvragen of die niet onterecht als besloten worden beschouwd, en waarvan behoeftestellers aangeven dat zij groot belang hebben bij het kunnen aftappen hiervan), en anderzijds kleine netwerkjes die volgens de letter van de wet openbaar lijken te zijn omdat zij Internettoegang faciliteren voor in beginsel eenieder, maar die eigenlijk fungeren als een besloten netwerk (waarvan sommigen zich afvragen of die niet onterecht als openbaar worden beschouwd). De verantwoordelijke instantie, OPTA, kan in deze gevallen momenteel de gevraagde duidelijkheid niet bieden, mede omdat het benodigde perspectief niet tot haar taak hoort.

3.3. Netwerken en diensten

Zowel netwerken als diensten?

Een belangrijke vraag is of moet worden vastgehouden aan het uitgangspunt dat zowel netwerken als diensten aftapbaar moeten zijn (par. 2.4.3). Het uitgangspunt stuit bij diverse aanbieders op kritiek. Hierbij spelen drie aspecten een rol.

In de eerste plaats wordt door diverse geïnterviewde aanbieders een onwenselijke overlap gesignaleerd. Diverse aanbieders van diensten, zowel bij telefonie als bij Internet, vinden het onnodig dat zij moeten aftappen wat op netwerkniveau goed aftapbaar is, zeker wanneer de dienst zelf niets toevoegt aan het verkeer als zodanig (bijvoorbeeld bij aanbieder(voor)keuze – carrier (pre)select). Ook zegt een netwerkaanbieder die tevens diensten aanbiedt dat hij het een desinvestering vindt om zijn netwerk aftapbaar te maken wanneer hij ook reeds al zijn diensten aftapbaar heeft gemaakt. Het ongeschreven uitgangspunt is dat de behoeftestellers eerst de dienstaanbieder aanspreken, en pas als die niet kan of wil meewerken de netwerkaanbieder. Dat laatste hoort volgens de wet niet voor te komen, maar dienstaanbieders kunnen niet altijd aftappen, bijvoorbeeld omdat zij geen beschikking hebben over alle nodige gegevens; een voorbeeld betreft de zogenoemde VMNO-aanbieders[105] van mobiele diensten, waarbij bijvoorbeeld inkomende sms-berichten niet via de centrales van de dienstaanbieder worden geleid. Behoeftestellers brengen daar tegenin dat zij in dergelijke gevallen een onderaannemingsovereenkomst moeten afsluiten met de netwerkbeheerder, om zo toch aan de plicht te voldoen. Voor de proportionaliteit van een tap is het immers belangrijk dat er op dienstniveau wordt getapt, en niet op netwerkniveau waarbij ook communicatie van niet-beoogde personen wordt meeonderschept.

Aangezien momenteel vaak netwerken en diensten bij één bedrijf zijn ondergebracht, is het onderscheid in de praktijk nog niet zo relevant voor de behoeftestellers, maar zij verwachten dat in de toekomst, bij toenemende ontbundeling van netwerken en diensten, vaker teruggegrepen zal moeten worden op het netwerk. Duidelijk is dat bij deze ontbundeling, in combinatie met het gelaagde telecommunicatieaanbod van netwerken, toegang en verscheidene toegevoegdewaardediensten, de verplichting om zowel netwerken als diensten aftapbaar te maken leidt tot behoorlijke overlap in aftapbaarheidscapaciteit.

In de tweede plaats merken dienstaanbieders, vooral bij Internet, op dat zij onevenredig zwaar worden getroffen door de aftapverplichting. Diensten zijn veelal eenvoudiger te ontwikkelen en op de markt te brengen dan netwerken; de verplichting om aftapbaar te zijn betekent bij diensten dan ook een relatief zwaardere belasting, zowel in kosten als in ontwikkeltijd. Daar komt bij dat onderdelen van de aftapverplichting, zoals beveiliging, met name voor kleine dienstaanbieders meer dan bij netwerkaanbieders een substantiële verandering van de inrichting van het bedrijf tot gevolg kan hebben (zie nader par. 6.1).

Hoewel het laatste punt duidelijk maakt dat de aftapverplichting voor dienstaanbieders evidente nadelen heeft, kan daaruit niet zonder meer worden geconcludeerd dat de verplichting in de

[105] Virtual Mobile Network Operators (VMNO's) maken vergaand gebruik van het GSM-netwerk van een andere aanbieder waarmee ze een overeenkomst zijn aangegaan. Slechts een relatief klein deel van het netwerk (waaronder bepaalde schakelcentrales en de klantbeheersystemen) bezitten zij zelf.

toekomst beperkt zou moeten worden tot netwerkaanbieders. De netwerkaanbieders kunnen immers vaak niet de benodigde af te tappen communicatie selecteren als er bijzondere diensten worden gebruikt, zoals chatgroepen of door derden opgezette VoIP-gesprekken. Ook weet een netwerkaanbieder vaak niet de identiteit(en) van de af te tappen gebruiker, en de behoeftestellers kunnen niet altijd tijdig alle identiteiten achterhalen (zie ook par. 4.2 en 7.3). In die gevallen kunnen netwerkaanbieders hooguit in bulk aftappen wat voorbij komt, waarbij de selectie van de af te tappen communicatie alsnog door behoeftestellers en/of dienstaanbieder moet gebeuren; dat maakt een veel ernstiger inbreuk op de privacy dan een selectieve tap op dienstniveau. De reden waarom in 1996 is gekozen voor aftapbaarheid van zowel netwerken als diensten, namelijk dat je niet alles kunt aftappen met of het een of het ander, vormt dan ook nog steeds een belangrijk argument om het uitgangspunt te handhaven.
Dit wordt versterkt door de voorkeuren die aanbieders in de vraaggesprekken aangaven: de ene dienstaanbieder vond dat alles op netwerkniveau moet worden getapt, maar de andere vond dat alleen diensten aftapbaar hoeven te zijn. Omgekeerd wilde de ene netwerkaanbieder ook dat alleen diensten zouden worden getapt, terwijl de andere netwerkaanbieder alles zelf wilde tappen ("omdat het ons netwerk is"). Een eenduidige keuze voor netwerken of diensten als voorwerp van de aftapplicht valt op basis hiervan dus niet te maken.

En welke netwerken en/of diensten?
Het is niet altijd duidelijk welke aanbieders van telecommunicatie aftapplichtig zijn, ook los van het vraagstuk van openbaarheid (par. 3.2). In de eerste plaats zijn er aanbieders 'aan de randen van de telecommunicatie'. Bijvoorbeeld aanbieders van toegevoegdewaardediensten, zoals informatiediensten op mobiele netwerken: de aanbieders hiervan staan nogal ver af van het traditionele type telecomaanbieder. Als bijvoorbeeld de ANWB en het KNMI dergelijke diensten aanbieden, vallen zij dan onder de Telecommunicatiewet en de aftapplicht?
Een ander voorbeeld betreft hostingaanbieders: diverse partijen gaven in de vraaggesprekken aan te denken dat deze onder de Telecommunicatiewet vallen, maar anderen, waaronder de behoeftestellers, gaven aan dat hosting-aanbieders niet onder de aftapbaarheidsplicht vallen. De wetgever heeft zich (pas) in maart 2005 laten ontvallen dat webhostingaanbieders niet openbaar zijn en dus niet onder de Telecommunicatiewet vallen. Het aftappen van hostingdiensten zal volgens het wetsvoorstel Computercriminaliteit II plaatsvinden zonder medewerking van de aanbieder.[106] Hoewel hier dus momenteel de wetgever duidelijkheid biedt, heeft er de nodige tijd rechtsonzekerheid bestaan over hostingaanbieders.
In de tweede plaats is niet altijd duidelijk wie nu precies aanspreekbaar is voor de eventuele aftapbaarheid. Bij glasvezelnetwerken is het beheer vaak verdeeld over verschillende partijen. WiFi-netwerken kennen vaak vrijblijvende organisatievormen zonder duidelijk centraal aanspreekpunt. Ook bij nieuwe telecommunicatiediensten is er in toenemende mate sprake van een samenwerkingsverband tussen verschillende partijen die elk een deel van de dienst voor hun rekening nemen, waarbij het niet evident is welke partij de precieze verplichting voor aftapbaarheid moet dragen. En ook al is het een wettelijke verplichting voor het consortium, het is voorstelbaar dat in dergelijke samenwerkingsverbanden partijen elkaar de bal zullen toespelen om de aftapbaarheid te regelen. Strakke handhaving zal dan nodig zijn om aftapbaarheid te kunnen garanderen, maar het zal er ook op aankomen dat duidelijk wordt gedefinieerd wat precies onder één (samenhangende) telecommunicatiedienst wordt verstaan en op welke manier die precies aftapbaar zal moeten zijn.

Conclusies over netwerken en diensten
Concluderend kunnen we stellen dat vraagtekens geplaatst worden bij de duale aftapbaarheidsplicht van netwerken én diensten, omdat een significante overlap dreigt wanneer aftapbaarheid verplicht blijft op alle lagen en in alle uiteinden van het steeds diverser wordende telecomlandschap. Hoewel de behoefte om beide te kunnen aftappen onverminderd is, worden de gevolgen van de aftapplicht wel groter, met name voor kleine dienstaanbieders die relatief veel grotere aanpassingen moeten plegen. Uit de reacties van gesprekspartners kan worden geconcludeerd dat de dualiteit eigenlijk voornamelijk op specifieke gebieden te legitimeren is, en dat de huidige eis van volledige dualiteit wel grote maatschappelijke kosten met zich meebrengt.

[106] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 24 en 26.

3.4. Nederland en buitenland

De aftapplicht geldt voor telecommunicatienetwerken en diensten die in Nederland worden aangeboden. Het gaat er dus om of een netwerk of dienst in Nederland wordt geleverd, niet waar een aanbieder is gevestigd.[107]
In de vraaggesprekken zijn geen problemen gesignaleerd rond buitenlandse aanbieders die in Nederland diensten aanbieden, met één uitzondering. Vaak is gewezen op buitenlandse aanbieders van grootschalige e-maildiensten. Diverse aanbieders hebben de indruk dat die in de praktijk niet aan de Nederlandse wetgeving rond aftapbaarheid worden gehouden, hetgeen zij als concurrentieverstoring ervaren (zie ook par. 6.6). Het aanbieden van grote opslagruimte aan e-mailgebruikers is immers duurder als deze dienst aftapbaar moet zijn, en kan daarom moeilijk concurreren met de buitenlandse aanbieders. De behoeftestellers wijzen er echter op dat aanbieders die in Nederland diensten aanbieden onder de Telecommunicatiewet vallen, en dat in dat kader afspraken worden gemaakt met buitenlandse aanbieders, zeker wanneer deze een Nederlandse vestiging of vertegenwoordiging hebben. Een probleem daarbij is wel dat met rechtshulpverzoeken moet worden gewerkt, omdat het om buitenlandse servers gaat, zodat deze weg alleen openstaat voor justitie maar niet voor ivd's.[108] Hoewel de aftapbaarheid van aanbieders die vanuit het buitenland opereren dus niet volledig kan worden gegarandeerd, is het momenteel geen groot knelpunt; 96% van de in Nederland aangeboden diensten wordt aangeboden door marktpartijen die vanuit Nederland opereren.
Een ander aandachtspunt is dat internationaal opererende bedrijven steeds vaker uit doelmatigheidsoverwegingen kiezen voor één internationaal platform om hun netwerken of diensten te ontwikkelen (zie ook par. 7.2), die dan vervolgens worden uitgerold in alle landen waar het bedrijf actief is.[109] Het moeten voldoen aan de specifieke Nederlandse wetgeving werkt dan belemmerend, omdat vanwege de relatief kleine markt geen aandacht is voor de Nederlandse situatie.

Concluderend kunnen we stellen dat er geen overwegende knelpunten zijn in aftapbaarheid bij het aanbod in Nederland van diensten vanuit het buitenland, mede omdat de markt grotendeels (nog) in Nederlandse handen is.

3.5. Conclusie

Het uitgangspunt dat openbare telecommunicatie aftapbaar moet zijn, staat niet ter discussie – ook aanbieders zijn het daarmee eens. Wel is een geschilpunt tussen aanbieders en behoeftestellers het moment waarop de aftapbaarheid gerealiseerd moet zijn. De behoeftestellers benadrukken dat telecommunicatie aftapbaar moet zijn 'vanaf het moment van introductie', maar dit wordt in de praktijk vaak niet gerealiseerd, en het doet onzes inziens ook geen recht aan de realiteit van de huidige telecommunicatiemarkt: bij vernieuwingen en technische actualiseringen kan lang niet altijd gewacht worden tot de aftapbaarheid volledig ingebouwd en getest is.
Over de mate waarin het uitgangspunt gerealiseerd wordt, kan op basis van de bevindingen van de vraaggesprekken worden geconcludeerd dat het overgrote deel van de openbare telecommunicatie grotendeels aftapbaar lijkt. Daarbij moeten de behoeftestellers soms wel genoegen nemen met voor hen suboptimale oplossingen, zoals het tappen op netwerkniveau omdat de dienst niet aftapbaar is, of tappen met enige vertraging omdat identificerende informatie van dienstgebruikers niet direct achterhaald kan worden. De behoeftestellers en de aanbieders verschillen van mening over hoe groot of hoe belangrijk het niet-aftapbare deel precies is. Niet-aftapbare delen worden onder meer veroorzaakt door een gebrek aan tijdige aftapspecificaties; behoeftestellers en aanbieders verwijten elkaar de oorzaak te zijn van dat probleem. Met name

[107] In deze paragraaf beperken we ons tot het aanbod vanuit het buitenland in Nederland. De vraagstukken rond het gelijke speelveld van verplichtingen in Nederland ten opzichte van verplichtingen in het buitenland komen aan bod bij concurrentieverstoring in par. 6.6.
[108] Daarbij wordt de wederzijdse rechtshulp gecompliceerd door het verschil in rechtscultuur tussen de VS en Nederland: in de VS moet zoveel mogelijk gefilterd worden om het tapmateriaal te beperken, terwijl dat in Nederland juist niet mag vanwege de volledigheid van het mogelijke (ook ontlastende) bewijsmateriaal.
[109] Bij een dergelijk platform kan worden gedacht aan een systeem waarop bijvoorbeeld WAP-diensten worden gerealiseerd, of de I-mode- of Live-diensten die KPN respectievelijk Vodafone aanbieden. Alle techniek wordt daarbij samengebracht, en de ontwikkeling vindt maar eenmaal plaats in één land, terwijl de desbetreffende dienst vervolgens in tientallen landen kan worden uitgerold.

bij kleine marktpartijen, zeker in de Internetwereld, bestaat een relatief groot wederzijds wantrouwen, dat maar moeizaam afneemt naarmate de partijen elkaar beter leren kennen. Het aftapbaar maken en houden is dan ook geen natuurlijk proces, maar een voortdurende bron van aandacht, zorg en regelmatig ook strijd. Uiteindelijk komen beide partijen er meestal wel uit, maar veelal pas na verloop van tijd en wellicht vaker met een gevoel van frustratie aan beide zijden dan met een gevoel van tevredenheid dat er weer een probleem is opgelost.

De huidige vormgeving van de aftapbaarheidsplicht als geldend voor alle openbare netwerken en diensten roept de nodige vragen op, veroorzaakt door de toenemende diversificatie van het telecomlandschap.
In de eerste plaats zijn er vragen rond het begrip openbaarheid. Aan de ene kant vallen de nodige kleine aanbieders met heel weinig gebruikers in beginsel onder de plicht omdat zij een openbare telecomdienst faciliteren, terwijl sommige grote aanbieders van netwerken of diensten met enorme aantallen gebruikers buiten de plicht vallen omdat zij (formeel) besloten gebruikersgroepen bedienen. Daar komt bij dat er in diverse gevallen onduidelijkheid bestaat over wat nu precies wel en niet openbaar is in, een onduidelijkheid die in de praktijk vaak niet wordt weggenomen. De vraag is dan ook of de verplichting van art. 13.1 TW in de toekomst moet blijven aanknopen bij het begrip openbaar, dan wel bij de invulling van dit begrip zoals dat wordt gehanteerd in de Telecommunicatiewet. Deze wet gaat over openbare telecommunicatie, met het doel de markt te ordenen; de behoefte om af te kunnen tappen staat los van dat marktordeningsperspectief, en verplichtingen voor besloten telecommunicatie, zoals in 13.7 TW, passen er ook helemaal niet in. Wellicht moet daarom worden overwogen om de aftapbaarheidsverplichting uit de Telecommunicatiewet te halen en in een aparte, zelfstandige Wet op de aftapbaarheid te plaatsen. Dan zou beter en effectiever kunnen worden bepaald voor welke netwerken en diensten de aftapbaarheidsplicht moet gelden, zonder dat men vastzit aan het begrip openbaarheid uit de Telecommunicatiewet.
In de tweede plaats kan het niet vanzelfsprekend zijn dat aftapbaarheid verplicht moet blijven op alle lagen en in alle uiteinden van het steeds diverser wordende telecomlandschap. Anders dan in 1996 of in 1998 zijn er nu veel meer aanbieders actief, waarvan een groot aantal kleine bedrijfjes zijn voor wie de verplichtingen relatief veel zwaardere lasten opleveren. De duale aftapbaarheidsplicht van netwerken én diensten dreigt een significante overlap op te leveren Hoewel de behoefte om beide te kunnen aftappen onverminderd is, worden de gevolgen van de aftapplicht wel groter, met name voor kleine dienstaanbieders die relatief veel grotere aanpassingen moeten plegen. Er kan echter niet zonder meer worden geconcludeerd dat het uitgangspunt van netwerken én diensten opgegeven moet worden. Aan het bezwaar van dreigende te grote overlap zou, als die overlap disproportioneel wordt gevonden, ook tegemoet kunnen worden gekomen door meer te differentiëren binnen netwerken en diensten naar gelang de specifieke behoeften van behoeftestellers en de mate waarin de niet-aftapbaarheid van het een opgevangen kan worden door de aftapbaarheid van het ander.

4. Meewerkplichten

4.1. Aftappen en verstrekken van verkeersgegevens

De verplichtingen van art. 13.2 en 13.2a TW tot het meewerken met bevelen tot aftappen en tot verstrekken van verkeersgegevens fungeren in de praktijk goed, vinden de aanbieders. Hoewel sommige aanbieders de bepalingen te summier vinden, waardoor hen niet duidelijk is in hoeverre ze precies waaraan moeten meewerken, noemen anderen de verplichtingen juist gedetailleerd genoeg en goed geformuleerd. Voor een nadere toelichting zouden sommige aanbieders het wenselijk vinden als er een centraal aanspreekpunt zou zijn bij de overheid dat kan uitleggen wat er precies wordt bedoeld.
De behoeftestellers vinden echter dat de meewerkplichten moeizaam lopen. De aanbieders van vaste- en mobieletelefonienetwerken zijn over het algemeen wel loyaal en geneigd om mee te werken,[110] maar Internetaanbieders staan volgens de behoeftestellers vijandig tegenover

[110] Waarbij aangetekend wordt dat bij deze bedrijven de afdeling die verantwoordelijk is voor het aftappen in een lastige tussenpositie zit; zij doen hun best mee te werken met de behoeftestellers, maar andere afdelingen binnen het bedrijf vinden die

aftappen. Hoewel lastgevingen zelden keihard worden geweigerd, is er vaak sprake van 'welwillende tegenwerking'.[111]

Rechtmatigheid en correctheid van de lastgeving
Een strijdpunt tussen enkele aanbieders en behoeftestellers is de beoordelingsmarge die deze aanbieders willen hebben om de lastgeving te beoordelen. Sommige aanbieders ervaren het als fundamenteel problematisch dat er geen specifieke rechtsgang open staat tegen een bevel tot meewerken,[112] omdat zij zich zorgen maken over eventuele aansprakelijkstelling[113] als achteraf zou blijken dat een bevel tot tappen of verkeersgegevensverstrekking onrechtmatig zou zijn.[114]
De behoeftestellers ervaren het echter als bijzonder storend dat aanbieders zichzelf een oordeel aanmatigen over de rechtmatigheid van een bevel. Zij kunnen en mogen niet voor rechter spelen en moeten een bevel gewoon opvolgen. Slechts bij evidente afwijkingen, zoals een handtekening met een duidelijk andere naam dan de genoemde bevoegde rechter, kan een aanbieder contact opnemen om uitleg te vragen. In de praktijk nemen sommige aanbieders echter veel meer beoordelingsruimte en stellen zij zich weigerachtig op.
De vraag of een aanbieder moet kunnen (laten) toetsen of een bevel op basis van een wettelijke bevoegdheid rechtmatig is gegeven, mede op basis van de Wbp-verantwoordelijkheid, is nog niet door rechtspraak of CBP beantwoord.[115] Het lijkt ons grotendeels een theoretische vraag: aanbieders zijn in de praktijk tot op heden nooit geconfronteerd met een aansprakelijkstelling voor een foute tap of gegevensverstrekking.
Belangrijker dan discussies over rechtmatigheid is dat vaak de correctheid van een lastgeving ter discussie staat. Soms zijn er simpele onduidelijkheden, zoals een niet bestaande identiteit (bijvoorbeeld een telefoonnummer met negen cijfers in plaats van tien) of een door herhaald heen en weer faxen onleesbaar geworden nummer, waarover dan overleg plaatsvindt. Het gebeurt echter ook regelmatig dat een aanbieder de kennelijke indruk heeft dat een verkeerd nummer (identiteit) wordt genoemd, bijvoorbeeld door – verondersteld – gebrekkige technische kennis aan de kant van een behoeftesteller; zij willen daarover dan in discussie gaan. Tijdens de vraaggesprekken hebben aanbieders diverse voorbeelden van taplasten genoemd waarin fouten voorkwamen.[116] Behoeftestellers ervaren de terugkoppeling van aanbieders echter vaak als storend en als een bewuste poging tot tegenwerken, vooral omdat aanbieders hier selectief mee om lijken te gaan. De aanbieder protesteert bijvoorbeeld niet als per ongeluk een IP-adres van de server van de aanbieder zelf in de taplast staat – dan voert de aanbieder die zonder morren uit in de hoop dat het justitiële systeem overbelast raakt.
Naar verluidt komen fouten in tapbevelen en gegevensvorderingen relatief vaak voor, vooral bij kleinere korpsen die minder ervaring hebben met aftappen en vaak over niet al te veel technische kennis beschikken.[117] Het CBP maakt momenteel een inventarisatie van dergelijke gevallen.
In de praktijk lossen de behoeftestellers en de aanbieders uiteindelijk dergelijke fouten wel samen op, maar discussies hierover scheppen wel wederzijdse spanningen.

Meerwaarde?
Is het nodig om aparte meewerkplichten in hoofdstuk 13 TW op te nemen, terwijl er toch al, impliciet of expliciet, meewerkplichten in het Wetboek van Strafvordering en de Wiv 2002 zijn

---

medewerking lang niet altijd vanzelfsprekend.
[111] De behoeftestellers gaven in het vraaggesprek een grove schatting dat ongeveer een derde van het aantal aanbieders consciëntieus zou meewerken, en rond tweederde zich opstelt met 'welwillende tegenwerking'.
[112] Anders dan de medewerking simpelweg te weigeren en een dagvaarding op basis van art. 184 Sr (niet-meewerken aan een bevoegd gegeven ambtelijk bevel) af te wachten.
[113] De aanbieder heeft immers op basis van de Wbp een verantwoordelijkheid om de gegevens van hun klanten te beschermen, die slechts doorbroken kan worden door een wettelijke plicht. Sommige aanbieders geven aan dat deze verantwoordelijkheid volgens hen betekent dat zij moeten kunnen beoordelen, of door een rechter moeten kunnen laten beoordelen, of er in een concreet geval daadwerkelijk sprake is van een wettelijke plicht, met name of een ambtelijk bevel voldoet aan de wettelijke eisen.
[114] Zie ook *Bijdrage van KPN aan de CBP expertmeeting Strafvordering in de Telecommunicatie,* KPN 2004.
[115] Dit is een van de vragen waar het CBP zich over buigt, naar aanleiding van een expertbijeenkomst 'Strafvordering in de telecommunicatie' in november 2004. Het Agentschap Telecom is overigens wel van mening dat aanbieders een beoordelingsmarge hebben: in het plaatje 'Hoe verloopt een internettap?' is een stap opgenomen 'Juridische Toets' die de ISP moet nemen alvorens tot de 'Technische Uitvoering' over te gaan, zie <http://www.agentschap-telecom.nl/informatie/aftappen/paginas/faq.html>.
[116] Een aanbieder vertelde dat eens een officier van justitie NAW-gegevens opeiste die hoorden bij een bedreigend e-mailbericht, niet van de afzender maar van de ontvanger (het slachtoffer), omdat de officier de header van het bericht verkeerdom las.
[117] Genoemd werden vooral fouten met tijdzones bij Internet; foute IP-adressen veroorzaakt door verkeerde tijdstempels of onduidelijk leesbare faxen waarin IP-adres en tijdstempel naadloos in elkaar overlopen; en interpretatiefouten (zoals het verwisselen van een nul en een O).

opgenomen? Art. 184 Wetboek van Strafrecht stelt immers het niet-meewerken aan een bevoegd gegeven ambtelijk bevel strafbaar.
Over de meerwaarde van zelfstandige meewerkplichten bestaat geen volledige eensgezindheid. Vele aanbieders vinden dat de bepalingen wel een meerwaarde hebben, omdat in Sv en de Wiv nu eenmaal geen uitvoerige telecommunicatiebepalingen kunnen worden opgenomen. Ook bieden ze helderheid en daarmee rechtszekerheid. De behoeftestellers vinden de zelfstandige plichten belangrijk, omdat ze meer handvatten bieden om medewerking af te dwingen, via het handhavingsbeleid van AT.
Aan de andere kant plaatsen sommigen wel vraagtekens bij de afstemming tussen Sv en Wiv enerzijds en TW anderzijds. Het zijn namelijk niet pure spiegelbepalingen, terwijl het dat volgens veel gesprekspartners wel zouden moeten zijn. Het CBP wees er in het vraaggesprek bijvoorbeeld op dat in het verleden art. 13.4 TW (zie nader par. 4.2) geen pendant kende in Sv – pas in 2004 zijn expliciete bevoegdheden om gebruikersgegevens op te vragen ingevoerd in het Wetboek van Strafvordering.[118] De Telecommunicatiewet kan aldus worden "misbruikt" om overheidsbevoegdheden te scheppen zonder dat daar de waarborgen tegenoverstaan die normaliter de bevoegdheden in het Wetboek van Strafvordering of de Wiv 2002 omkleden, zoals notificatie (art. 126bb Sv). Ook gaf een aanbieder aan dat het in de praktijk soms voorkomt dat een behoeftesteller hem beveelt om mee te werken op basis van hoofdstuk 13 TW, zonder verwijzing naar de relevante bevoegdheid uit Sv.
Desondanks kan op basis van de bevindingen van het onderzoek wel worden vastgesteld dat men over het algemeen vindt dat de meewerkplichten in hfd. 13 TW een meerwaarde hebben, en dat deze volgens de meesten wel als spiegelbepalingen fungeren met de bevoegdheden in Sv en de Wiv.

Concluderend kan gesteld worden dat de meewerking tussen aanbieders en behoeftestellers niet altijd vlekkeloos verloopt; met de aanbieders van telefonienetwerken bestaan betere contacten en vertrouwensbanden dan met Internetaanbieders of nieuwe dienstaanbieders. Niettemin wordt er uiteindelijk wel bijna altijd meegewerkt. De formulering van de meewerkplichten in hoofdstuk 13 heeft in dat opzicht ook een meerwaarde, aangezien ze bij onwelwillende aanbieders een extra stok achter de deur vormen. Een relevante open rechtsvraag is wel in hoeverre aanbieders een beoordelingsmarge hebben om meewerking te weigeren als zij de indruk hebben dat een lastgeving onbevoegd is gegeven of fouten bevat; er is behoefte aan meer duidelijkheid hierover.

4.2. Gebruikersgegevens en CIOT

De meewerkplicht tot verstrekking van gebruikersgegevens, art. 13.4 TW, fungeert momenteel wat anders dan de hiervoor besproken meewerkplichten voor tappen en verkeersgegevens.[119] De verstrekking gebeurt namelijk via het CIOT, het Centraal informatiepunt onderzoek telecommunicatie, een centrale databank waaraan telecommunicatieaanbieders iedere 24 uur een geactualiseerd bestand van gebruikersgegevens beschikbaar moeten stellen (zie par. 2.5.4). Momenteel is het CIOT beperkt tot telefonie, waarop in paragraaf 4.2.1 wordt ingegaan. Vervolgens behandelen we de in de nabije toekomst voorziene uitbreiding van het CIOT met Internet-gegevens (par. 4.2.2).

4.2.1. Telefonie

CIOT
Het CIOT functioneert, volgens zowel aanbieders als behoeftestellers, sinds ongeveer een jaar naar tevredenheid (in elk geval sinds de formele inwerkingtreding per 1 september 2004). Voorheen liep de verstrekking via individuele aanbieders, en daarvoor gold min of meer hetzelfde als hierboven (par. 4.1) is geconstateerd, met de complicatie dat de overheidsbevoegdheden om

[118] Voorheen konden NAW-gegevens alleen worden verkregen als verkeersgegevens werden gevorderd op basis van art. 126n/u Sv (art. 125f-oud), waarbij *en passant* de gebruikersgegevens werden meegeleverd; gebruikersgegevens konden dus alleen worden opgevraagd in relatie tot concrete belhandelingen, maar niet als zelfstandige gegevens. Een ander voorbeeld is de IMSI-vanger, geregeld in art. 3.10 TW, die lange tijd geen spiegelbepaling kende in Sv; deze werd pas bij wet van 5 april 2001, Stb. 180, ingevoerd als strafvorderlijke bevoegdheid in art. 126na/ua-oud Sv (nu art. 126nb/ub Sv).
[119] Het CBP wees er in het vraaggesprek op dat het onderscheid tussen gebruikersgegeven en verkeersgegeven momenteel niet scherp genoeg is. Het begrip nummer is bij de totstandkoming van de TW geïnterpreteerd als ook omvattend nummers waarnaar is doorgeschakeld (wat meer een verkeersgegeven lijkt te betreffen), en nummers van basisstation (terwijl de locatie een verkeersgegeven is).

gebruikersgegevens op te vragen lange tijd niet of onduidelijk geregeld waren in de daarvoor bestemde wetten;[120] art. 13.4 lid 1 TW kende in die periode dus geen spiegelbepalingen in Sv of Wiv, waardoor aanbieders eerder (maar lang niet altijd) hun medewerking weigerden.
Hoewel de oprichting van het CIOT al in 1996 was voorzien en in de TW van 1998 was opgenomen, en de AMvB ter uitvoering daarvan in januari 2000 werd gepubliceerd, is het orgaan pas op 1 september 2004 in werking getreden. Daarvoor fungeerde het CIOT al wel op basis van een convenant uit 2001. Het CBP vond dit bezwaarlijk; het is een voorbeeld van een 'pro-actieve' bevoegdheidsuitoefening zonder adequate wettelijke basis.[121] De meeste geïnterviewde aanbieders vonden die eerdere uitvoering niet problematisch, en zij gaven aan veel van de benodigde gegevens geleverd al in een vroege fase te hebben. De behoeftestellers vinden echter dat het in de aanloopjaren amper gewerkt heeft, en stellen dat uiteindelijk slechts een overeenkomst over de proefproductiefase tot stand kwam, maar dat het convenant nooit ondertekend is geweest.
Medeoorzaak van de late inwerkingtreding was een kip-ei-constructie die in het *Besluit verstrekking gegevens telecommunicatie* zat ingebakken: het besluit kon pas in werking treden als alle aanbieders waren aangesloten, maar (sommige) partijen sloten zich niet aan zo lang het besluit nog niet in werking was. Deze patstelling is nu in elk geval doorbroken, en het CIOT wordt over het algemeen als een uitstekende constructie ervaren. Aanbieders noemen het ook een verbetering ten opzichte van de oude situatie.
Inmiddels is het CIOT grotendeels dekkend, met ruim 90% van alle nummers. Het niet-opgenomen deel bestaat uit afgesloten telefoonnummers, nummers behorend bij niet-aangesloten aanbieders, en een uiteenlopende categorie ontbrekende nummers samenhangend met technische fouten en tekortkomingen. De dekking is hiermee sterk toegenomen ten opzichte van 2002 (ongeveer 50%) en 2004 (ongeveer 80%), omdat sindsdien veel aanbieders zijn toegetreden, vele beltegoednummers (*pre-paid*) zijn als zodanig toegevoegd zodat de behoeftesteller ten minste weet dat hij met een beltegoednummer te maken heeft als de aanbieder niet over NAW-gegevens beschikt, en een substantiële categorie ISDN-30 is toegevoegd.[122] De opname van beltegoednummers is een vooruitgang, omdat aanbieders voordien relatief vaak werden geconfronteerd met een aan alle aanbieders verzonden vraag of een desbetreffend nummer bij hen in gebruik was; nu weten behoeftestellers tenminste gelijk dat het een beltegoednummer betreft.[123] Overigens melden sommige aanbieders dat zij sowieso soms verzocht worden om gebruikersgegevens te leveren zonder dat het CIOT is geraadpleegd; dit zijn echter volgens de behoeftestellers uitzonderlijke gevallen. En aanbieders kunnen, aldus het CIOT, simpelweg het verzoek afwijzen, omdat de afspraak is vastgelegd dat behoeftestellers alleen rechtstreeks een aanbieder mag vragen om gebruikersgegevens onder overlegging van een 'niet aangetroffen'-verklaring ('no hit') van het CIOT.
Hoewel er een hoge dekkingsgraad is van de in gebruik zijnde telecomnummers, zijn nog diverse aanbieders – met een relatief klein marktaandeel – niet aangesloten op het CIOT. Sommige aanbieders vinden dat zij er niets mee te maken hebben, omdat zij als niet rechtstreeks met telecomgebruikers te maken hebben en de feitelijke diensten uitbesteden; aan de andere kant kan worden gesteld dat zij nu eenmaal wettelijk verplicht zijn om mee te werken, en dus maar moeten regelen, zelf of met eventuele andere aanbieders, om klantgegevens naar het CIOT te geleiden. Andere aanbieders lijken om andere redenen onwillig om zich aan te sluiten – wellicht speelt hierbij soms een – al dan niet gesimuleerde – gebrekkige kennis van de wet een rol ("wij hebben toch alleen zakelijke klanten?"). In de praktijk worden de probleemgevallen meestal aangepakt in onderling contact tussen het Ministerie van Justitie en de desbetreffende aanbieder, al blijft het CIOT zelf de doorlooptijd van aansluiting wel als een knelpunt ervaren.

Aandachtspunten
Diverse aanbieders signaleren het risico dat de gegevens uit het CIOT op foute wijze worden gebruikt, omdat de gegevens geen 'historisch besef' hebben.[124] Dat kan tot foute interpretaties

[120] Voor justitie werd de bevoegdheid gebruikersgegevens te vorderen ingevoerd in art. 126n, 126na, 126u en 126ua Sv per 1 september 2004; voor de ivd's werd art. 29 Wiv 2002 per 29 mei 2002 ingevoerd.
[121] Het CBP heeft destijds overigens wel ingestemd met het convenant, vooruitlopend op de uiteindelijke formele wettelijke regeling.
[122] ISDN-30 is een type aansluiting waarbij tot dertig gelijktijdige telefoonverbindingen kunnen worden aangeboden. Dit wordt veel gebruikt voor het aansluiten van bedrijven, die er vervolgens de eigen bedrijfstelefooncentrale op aansluiten.
[123] Dat betekent niet direct dat de behoeftestellers dan ook te weten komen wie er achter het nummer steekt, omdat veel prepaid-gebruikers zich niet registreren bij de aanbieder.
[124] De gegevens worden immers elke 24 uur overschreven met nieuwe gegevens. Het CIOT bevat alleen een momentopname van

leiden, bijvoorbeeld wanneer justitie een zes maanden oud en inmiddels overgedragen mobiel nummer gebruikt om NAW-gegevens op te vragen, en vervolgens op de verkeerde plaats een doorzoeking zou uitvoeren. Opsporingsambtenaren moeten zich bewust zijn van dit risico. Het terzijde stellen van de kennis van de aanbieder, die bij een gegevensverzoek wel kan zien of een telefoonnummer recentelijk van gebruiker is veranderd, wordt wel als een nadeel beschouwd van de CIOT-constructie.
Een ander aandachtspunt bij het CIOT, genoemd door de behoeftestellers, is dat er wel informatie over de klanten wordt aangeleverd, zoals telefoonnummer en NAW-gegevens, maar dat het zogenoemde dienstenveld niet adequaat is geregeld. Aanbieders nemen vaak niet op of het een ISDN- of faxaansluiting is, of dat iemand GSM of UMTS gebruikt. Hierdoor wordt het uitvoeren van een tap bemoeilijkt. Bij de opzet van het CIOT is daar niet goed over nagedacht, maar hier wordt inmiddels wel aan gewerkt.

Bewerkersovereenkomst
Een laatste kritiekpunt op het CIOT betreft de bewerkersovereenkomst die noodzakelijk is, omdat de Wbp een dergelijke overeenkomst eist indien een verantwoordelijke voor persoonsgegevens (in casu de aanbieder) gegevens laat bewerken door een ander (in casu het CIOT). Het CIOT heeft lang gewerkt zonder dat er bewerkersovereenkomsten met de aanbieders waren afgesloten;[125] inmiddels zijn die er wel, maar deze worden als onvoldoende beschouwd en het model ervoor wordt momenteel herzien.[126] Sommige aanbieders ervaren het ook als problematisch dat zij de gebruikersgegevens uit handen moeten geven zonder enige controlemogelijkheid op hoe deze vervolgens worden gebruikt, terwijl zij wel verantwoordelijke zijn in de zin van de Wbp. Of de bewerkersovereenkomst dit punt, en de daarmee samenhangende aansprakelijkheid, adequaat regelt, kwam niet duidelijk naar voren uit de vraaggesprekken. Men vindt het in ieder geval wel van belang dat er adequaat toezicht is op het gebruik van het CIOT, in de vorm van een periodieke controle op het systeembeheer.

Concluderend kunnen we stellen dat het CIOT, als uitwerking van art. 13.4 lid 2 TW, naar tevredenheid functioneert en een van de meest geslaagde onderdelen van het aftapbaarheidsbeleid lijkt.[127] Het wordt een intelligent opgezet en efficiënt systeem gevonden met de nodige ingebouwde *checks and balances*; het gebrek aan historisch besef van de gegevens is een nadeel maar ook een bewust ingebouwde beperking. Wat wel beter geregeld kan worden zijn de verplichting om diensten aan te duiden en – waar aan gewerkt wordt – de bewerkersovereenkomst.

4.2.2. Uitbreiding met Internet

Zoals in par. 2.5.4 vermeld, hoeven Internetaanbieders nog niet mee te werken met het CIOT. De ontheffing geldt volgens art. 12 lid 2 van het *Besluit verstrekking gegevens telecommunicatie* tot 1 september 2006. Momenteel loopt een proefproject met drie aanbieders om ervaring op te doen met Internetgegevens in het CIOT. De NLIP gaf in het interview aan blij te zijn dat er samen met marktpartijen een haalbaarheidsonderzoek wordt gedaan; het is een indicatie dat beseft wordt dat Internet iets anders is dan telefonie en dat deze verschillen ook gevolgen kunnen hebben voor een systeem als het CIOT. Wel uitten sommigen de vrees dat door het beperkte aantal aanbieders dat betrokken is bij het proefproces een uitkomst kan opleveren die, gezien de grote diversiteit aan soorten Internetaanbieders en de interne systemen die zij hanteren voor klantregistratie, voor andere aanbieders minder werkbaar zal zijn. Ook werd opgemerkt dat de nodige aanbieders ook geen gecentraliseerd klantenbestand hebben. Aan de andere kant wordt gesteld dat de verplichting nu eenmaal vastligt, en dat het voor aanbieders hooguit een eenmalige operatie is om de registratie van klantgegevens in het benodigde formaat om te zetten.

---

de dan in gebruik zijnde telecommunicatienummers.
[125] Het CBP uitte in het vraaggesprek kritiek op de late totstandkoming van de bewerkersovereenkomst; volgens een gesprekspartner van de overheid signaleerde het CBP echter zelf deze problematiek aan de late kant.
[126] Het CBP heeft bij brief van 14 februari 2005 (kenmerk z2003-1358) bij het Ministerie van Justitie aangedrongen op een nieuwe bewerkersovereenkomst, onder andere in verband met het feit dat het CIOT ook zelf gegevens opslaat.
[127] Dat het systeem voor de huidige functie goed functioneert betekent niet per se dat deze aanpak zonder meer voor andere gebieden geschikt is (zie par. 4.2.2).

Het voornaamste knelpunt bij de uitbreiding met Internetgegevens is de veel grotere dynamiek in adressering die op het Internet plaatsvindt (zie nader par. 7.3). Dynamische IP-adressen, maar ook de mogelijkheid om elke minuut een ander alias van een e-mailadres te kiezen, maken dat een actualisering van eens per 24 uur de nodige gegevens zal missen. Om zeker te weten welk – dynamisch – aansluitnummer bij welke klant hoort, zal het nodig zijn om bij deze gegevens een tijdstempel te bewaren, dat aangeeft van hoe laat tot hoe laat het bij wie in gebruik was. Dat geeft het "Internet-CIOT" een ander karakter dan het "telefoon-CIOT", omdat nu ook historische gegevens worden opgeslagen; het huidige CIOT daarentegen kent geen geheugen. De behoeftestellers geven aan dat dit niet gezien moet worden als het verzamelen van historische gegevens, maar als het achterhalen van identiteiten. Dat is strikt genomen juist, maar het eerste is wel een direct uitvloeisel van het tweede. Een belangrijk vraagpunt zal dan ook zijn hoe lang de tijdgestempelde gegevens bewaard zouden moeten worden. Aanbieders merken daarbij ook op dat dit soort gegevens normaliter niet worden vastgelegd, of in elk geval niet systematisch en met grote gaten of foutpercentages erin, omdat de aanbieder geen belang heeft bij vastlegging;[128] een registratieplicht leidt dus tot hogere opslagcapaciteit maar ook tot scherpere controlenoodzaak en daarmee tot hogere kosten.
Overigens geven behoeftestellers aan dat zij gebruikersgegevens in beginsel steeds direct nodig hebben, met name om een tap te kunnen plaatsen. Het heeft dan weinig zin om van het CIOT te horen dat gisteravond tussen 21:30u en 21:35u de verdachte een bepaald IP-adres in gebruik had – nodig is te weten welk dynamisch IP-adres nu in gebruik is. Dat valt feitelijk alleen te doen met een directe, geautomatiseerde toegang tot de actuele gegevens van de Internetaanbieders. Dat is evenwel een fundamenteel ander systeem dan het CIOT.
Al met al zijn er de nodige cruciale vragen en kanttekeningen te plaatsen bij de nakende uitbreiding van het CIOT met Internetgegevens. Het wordt door velen betwijfeld of de datum uit het besluit, 1 september 2006, haalbaar is. Verwacht wordt dat het besluit zal moeten worden aangepast, niet alleen vanwege de datum maar ook omdat meer dingen geregeld zullen moeten worden die nog moeten worden beslist. Daarbij plaatsen sommigen, waaronder het CBP, principiële vraagtekens bij de transponering van bestaande telefonieregels naar Internet, omdat het om fundamenteel verschillende systemen gaat waarbij het lang niet altijd proportioneel is om de regels van het ene systeem zonder meer naar het andere over te hevelen.[129]

4.3. Beperkte bewaarplicht

Art. 13.4 lid 2 TW kent een beperkte bewaarplicht voor telefonieaanbieders, namelijk gedurende drie maanden voor de gegevens nummer, tijd en basisstation bij bellers met vooruitbetaalkaarten (zie par. 2.5.5). Deze bewaarplicht wordt door aanbieders niet als een probleem ervaren; diverse aanbieders geven aan dat ze deze gegevens toch al voor deze duur (of langer) bewaren voor interne doeleinden.[130]
Ook de behoeftestellers vinden dat de bewaarplicht goed nageleefd wordt. In de praktijk blijken de opgeslagen gegevens echter niet te worden gebruikt voor het doel waarvoor de bewaarplicht is ingevoerd, namelijk bestandsvergelijking om gebruikersgegevens van vooruitbetaaltelefonie te achterhalen. In tegenstelling tot een principeafspraak om de gegevens binnen twee uur te leveren, blijken aanbieders niet snel genoeg deze gegevens kunnen achterhalen, aldus de behoeftestellers. In dergelijke gevallen zou de behoeftesteller dan zijn toevlucht moeten nemen tot de IMSI-vanger (zie par. 2.5.5) om het aansluitnummer van een af te tappen persoon te achterhalen. Van de bewaarplicht hoeft dan geen gebruik worden gemaakt.
Daarnaast constateren behoeftestellers dat de meeste aanbieders in de praktijk weigeren een bestandsvergelijking uit te voeren, omdat zij vinden dat dit niet hun taak is maar een opsporingstaak. Bovendien worden er soms mensen gevolgd die vanuit het buitenland naar Nederland komen; over hen zijn geen gegevens bekend bij de Nederlandse aanbieders. In dat geval levert de bewaarplicht geen bruikbare gegevens op en is wederom de IMSI-vanger een bruikbaar alternatief.

[128] Vgl. Stratix, *Onderzoek "Bewaren Verkeersgegevens door Telecommunicatieaanbieders. Eindrapport*, Schiphol, augustus 2003 beschikbaar via <http://www.justitite.nl>, p. 33: 'Bij sommige ISP's blijkt in de praktijk zelfs tot 10% van de RADIUS sessiegegevens verloren te gaan als gevolg van het ontbreken van een overdrachtscontrole in dit protocol.'
[129] We gaan hier niet verder in op de ook geuite zorgen dat het CIOT-systeem geleidelijk aan uitgebreid zal worden met verkeersgegevens of met gegevens uit andere sectoren. Dit valt buiten het bestek van het onderzoek.
[130] Eén aanbieder merkte daarbij op dat gespreksgegevens 1 tot 2 jaar bewaard worden, maar dat de duurzaamheid van de gegevens echter niet wordt gegarandeerd, vanwege de beperkte houdbaarheid van de drager (tape).

Men kan dus concluderen dat de beperkte bewaarplicht weliswaar wordt uitgevoerd, maar niet het beoogde doel dichterbij brengt.

4.4. Conclusie

Op basis van de bevindingen constateren wij dat de medewerking van aanbieders met lastgevingen van behoeftestellers voor een deel van de markt redelijk tot goed en voor een ander deel minder goed verloopt. Overigens wordt er uiteindelijk wel meestal meegewerkt, zij het wel met de nodige spanningen. Uit de gevoerde gesprekken ontstaat de indruk dat beide kanten wel eens steken laten vallen – de behoeftestellers bijvoorbeeld bij fouten in lastgevingen of benadering van de verkeerde personen, en de aanbieders bijvoorbeeld door niet te melden als relevante gegevens (bijvoorbeeld aansluitnummers) veranderen terwijl die op dat moment onder een tap staan. Dergelijke voorvallen maken de onderlinge verhouding er niet beter op.

In dit licht lijkt de formulering van meewerkplichten in art. 13.2, 13.2a en 13.4 TW wel een meerwaarde te bieden ten opzichte van de verplichtingen die toch al bestaan op basis van de Wetboeken van Strafvordering en Strafrecht en de Wiv 2002. Bij al dan niet moedwillige tegenwerking door aanbieders vormen deze bepalingen een extra stok achter de deur.
Over het geheel genomen zijn de meewerkplichten ook adequaat geformuleerd en toereikend. Enkele kanttekeningen zijn dat het onduidelijk is in hoeverre aanbieders meewerking mogen weigeren als zij reden hebben te vermoeden dat een lastgeving onjuist is en dat de beperkte bewaarplicht van art. 13.4 lid 2 niet wordt gebruikt om het beoogde doel van identificatie van vooruitbetaalbellers te bereiken.

5. Kosten en kostenverdeling

5.1. Investeringskosten

Uitgangspunt: investeringskosten voor de aanbieder
Art. 13.6 TW bepaalt dat de investeringskosten voor het aftapbaar maken en houden voor rekening van de aanbieder komen. Hiervoor is destijds een politieke keuze gemaakt (zie par. 2.6.1).

De behoeftestellers zijn het eens met deze keuze en vinden ook dat dit uitgangspunt gehandhaafd moet blijven. Het leggen van investeringskosten bij de aanbieders is en blijft volgens hen de beste garantie dat een kosteneffectieve oplossing wordt gekozen, omdat de overheid niet kan controleren welke investeringskosten precies nodig zijn voor aftapbaar maken. In de praktijk is ook een zekere marktwerking te zien geweest bij leveranciers van aftapapparatuur, mede onder druk van aanbieders om de kosten omlaag te brengen. De behoeftestellers trekken ook een parallel met tal van wettelijke verplichtingen die kosten opleveren voor bedrijven, bijvoorbeeld om te voldoen aan ARBO- of veiligheidswetgeving. Aanbieders zijn – weinig verrassend – minder enthousiast over het uitgangspunt. Zij noemen aftappen een taak voor de opsporing, niet voor het bedrijfsleven, en aftapbaarheid in het verlengde daarvan een overheidsverplichting. Tegenover het argument van de kostenbeheersing stellen aanbieders dat het juist doelmatiger is als de overheid de investeringen zou betalen, omdat zij dan bewust zou investeren in netwerken en diensten die zij vervolgens ook daadwerkelijk gaat aftappen, terwijl nu investeringen worden gepleegd terwijl er lange tijd geen gebruik wordt gemaakt van de aftapbaarheid. Daarnaast wordt ook wel opgemerkt dat de huidige kostenverdeling mede het resultaat is van het overleg dat in de jaren negentig is gevoerd tussen overheid en de toenmalige, grote marktpartijen, waarbij de marktpartijen uiteindelijk de aftapverplichting en daarmee gepaard gaande investeringen voor lief namen omdat zij niet wilden dat de overheid zelf op hun netwerken zou gaan tappen. De nieuwe, kleine aanbieders die sindsdien op de markt zijn gekomen, zouden misschien een andere afweging willen maken als zij tussen deze Skylla en Charybdis zouden moeten kiezen.

Niettemin kan wel worden vastgesteld dat de meeste aanbieders zich in de praktijk hebben neergelegd bij het uitgangspunt.[131] Dat geldt overigens niet voor XS4ALL, die het uitgangspunt in het vraaggesprek 'bizar' noemde en die op 7 maart 2005 de Nederlandse staat heeft gedagvaard om de investeringskosten terug te vorderen.[132] De uitkomst van dat proces kan belangrijke gevolgen hebben voor de kostenverdeling, maar naar verwachting kan het vele jaren duren voor er een definitieve uitspraak is, aangezien het een civiele bodemprocedure betreft.

Feitelijk gemaakte kosten
Gevraagd naar de feitelijke investeringen die gepleegd zijn, geven de aanbieders aan dat deze kosten niet apart worden bijgehouden. Een dergelijke registratie kost veel inzet en dient vooralsnog geen specifiek doel (zie kader 5.1). Desalniettemin gaat het volgens de aanbieders niet alleen om grote bedragen – zij noemen soms bedragen in de orde van honderdduizenden tot enkele miljoenen euro's –,[133] maar ook om substantiële percentages van de totale investeringskosten in onderzoek en ontwikkeling. Veel aanbieders refereerden aan de in de jaren '90 herhaaldelijk gedane uitspraak van de minister en staatssecretaris dat de investeringskosten niet meer dan 1% van de totale investeringen zouden vergen (zie par. 2.6.1). Hoewel slechts enkele aanbieders concrete percentages noemden, die veel hoger liggen dan 1%,[134] gaven vrijwel alle geïnterviewde aanbieders aan dat 1% een veel te lage schatting is. Aangezien het onderhavige onderzoek zich beperkte tot interviews en geen bedrijfseconomisch onderzoek bevatte, kunnen de bedragen en percentages niet worden getoetst, en bovendien zijn de investeringskosten sowieso moeilijk exact te bepalen (zie kader 5.1). De onderzoekers hebben niettemin de indruk dat, hoe gekleurd de beweringen van de aanbieders ook kunnen zijn, de benodigde investeringen voor nieuwe netwerken of diensten wel zeker substantieel meer zijn dan de door de wetgever genoemde 1%. Dat geldt zeker voor kleinere dienstaanbieders, omdat de systemen voor aftapbaarheid maar deels schaalbaar zijn en er altijd sprake is van een fors startbedrag[135]. De wetgever had in de jaren negentig ook dergelijke aanbieders niet voor ogen, omdat er toen alleen grotere netwerkaanbieders op de markt waren, waarbij de investeringskosten voor de fysieke infrastructuur sowieso vrij hoog liggen. Hier moet worden opgemerkt dat een aantal kleinere aanbieders gebruik maakt van de aftapvoorziening van het NBIP en zo bepaalde delen van haar investeringskosten weet te beperken (zie par. 2.4.1). Dit geldt echter slechts voor een deel van de benodigde interfaces; andere voorzieningen moet elk van de aanbieders die aangesloten is bij het NBIP zelf aanbrengen. Zoals boven aangegeven wordt over een aftapvoorziening zoals het NBIP door vrijwel alle betrokkenen positief geoordeeld; om diverse redenen is een dergelijke opzet echter alleen passend bij relatief kleine aanbieders.[136]

Daar komt bij dat veel aanbieders opmerken dat het aftapbaar *houden* van hun infrastructuur vaak meer kosten met zich meebrengt dan aanleg van de initiële voorzieningen. Regelmatig worden veranderingen in het netwerk aangebracht met als doel de capaciteit te vergroten, nieuwe diensten te introduceren of het netwerk kostenefficiënter te maken. Bij elk van die veranderingen moet opnieuw gekeken worden of de aftapvoorziening nog goed functioneert en of eventuele wijzigingen moeten worden aangebracht. Ter illustratie: leveranciers van verkeerscentrales voor

[131] Zoals de behoeftestellers terecht opmerkten in het vraaggesprek: de voorspelling die aanbieders in de jaren negentig deden dat de komende investeringsverplichtingen aanbieders naar het buitenland zou doen uitwijken, is allerminst uitgekomen.
[132] Zie <http://www.xs4all.nl/nieuws/bericht.php?taal=nl&id=616&msect=nieuws> en <http://www.xs4all.nl/nieuws/pdf/XS4ALLdagvaarding.pdf>.
[133] Het enige publiek bekend gemaakte cijfer is 'méér dan 1 miljoen gulden' die XS4ALL in zijn privacyverslag over de periode 1/1/2003-30/6/2004 noemt, zie <http://www.xs4all.nl/overxs4all/privacy/privacy_jaarverslag.html>. Opmerkelijk is de opmerking in het verslag: 'Per abuis stond het bedrag aan investeringskosten eerder weergegeven in euros in plaats van guldens.' Het feit dat in guldens wordt gerekend suggereert dat het bedrag niet de jaarverslagperiode betreft maar de totale cumulatieve kosten (dan wel dat een andere rekeneenheid is gehanteerd om "meer dan een miljoen" te kunnen noemen?). Andere aanbieders noemden in gesprekken bedragen van honderdduizenden tot enkele miljoenen euro's.
[134] Eén aanbieder gaf een voorbeeld van een dienst waarbij de aftapbaarheid rond de 20% van de totale investeringen kostte. Een andere, kleine, aanbieder noemde een percentage van 30% van de totale netwerkinvesteringen. Zie ook de brief van de Raad van de Centrale Ondernemingsorganisaties aan de staatssecretaris van EZ, van 7 maart 2003, waarin een percentage wordt vermeld van 5 tot 40% van de totale investeringskosten, <http://www.nuv.nl/web/show/id=101644/dbcode=374/filetype=letters>. De NLIP gaf in een schriftelijk vervolg op het vraaggesprek aan de onderzoekers aan dat in 'de praktijk blijkt dat de kosten voor het technisch aftapbaar maken van de netwerken, zeker in het begin substantieel, en daarna onevenredig veel hoger zijn dan in het beleidsuitgangspunt is voorzien'.
[135] Er is bijvoorbeeld voor bepaalde gevallen alleen apparatuur voorhanden die een capaciteit heeft voor 50 simultane taps, terwijl sommige kleine aanbieders hooguit één of twee taps tegelijk hebben lopen.
[136] Dat heeft diverse redenen. Zo neemt naarmate de aanbieder groter is de kans toe dat er op een bepaald moment in de tijd één of meerdere taps lopen. Daarmee wordt de bezettingsgraad groter en neemt de ratio van het delen van voorzieningen af.

mobiele netwerken (de zogenaamde MSC's) brengen jaarlijks nieuwe revisies ('upgrades') uit van de systeemsoftware. Om allerlei redenen kan een operator zich gewoonlijk niet permitteren een revisie over te slaan. Bij elke installatie vragen de aftapvoorzieningen echter weer om aandacht, zeker omdat er in Nederland voor een afwijkend systeem is gekozen (ETSI-NL en TIIT, zie par. 2.4.4). Dit werkt kostenverhogend (zie par. 3.1).
Een andere kostencategorie die diverse aanbieders noemen is dat zij niet alleen investeren in aftapbaarheidsvoorzieningen, maar ook de nodige menskracht investeren in het ontwikkelen van modellen en specificaties voor aftapbaarheid bij nieuwe netwerken of diensten, zoals TIIT, terwijl het een overheidsverantwoordelijkheid is om die specificaties aan te leveren. Zij vinden het onterecht dat zij daarin moeten investeren. Anderzijds moet ook worden geconstateerd dat aanbieders tegelijkertijd ook juist betrokken willen zijn bij de ontwikkeling van deze specificaties, omdat hen dit enige speelruimte geeft. Een eigen investering lijkt dan niet misplaatst.

Voor aanbieders is het vaak lastig om vast te stellen hoeveel er nu feitelijk is uitgegeven om aan de aftapverplichting te voldoen. Dat komt omdat het veelal om niet-verbijzonderde uitgaven gaat. Omdat er momenteel geen noodzaak toe is, houden aanbieders momenteel niet bij welke kosten precies aan aftappen toegerekend kunnen worden.
De directe kosten in de vorm van specifiek aangekochte systemen en software ten bate van aftapbaarheid zijn voor veel bedrijven nog wel goed in kaart te brengen. Al wat lastiger is het aandeel van de kosten in de systemen binnen het netwerk zelf. Het is niet eenvoudig op te maken wat het kostenverschil is met een netwerkuitrol welke aftappen niet ondersteund (versies zonder aftapvoorzieningen worden niet uitonderhandeld). Maar indien nodig zullen dergelijke kosten vermoedelijk ook nog wel zichtbaar kunnen worden gemaakt. Nog moeilijker te kwantificeren kosten liggen er bij allerlei processen, variërend van dienstenontwerp, *procurement*, revisie(management), infrastructuuropwaarderingen, upgrades in het basisnetwerk, enz, enz. Bij al deze zaken vraagt het onderwerp aftapbaarheid om aandacht in de vorm van aan te kopen apparatuur, benodigde feature sets van apparatuur, ontwerp en architectuur van netwerk en diensten, alsmede het testen.
Het komt er kortom op neer dat bijna alle bedrijven de aftapvoorzieningen en alles wat daar mee te maken heeft, als (noodzakelijke) overhead beschouwen. De terugkerende exercitie om deze kosten te kwantificeren zal niet leiden tot besparingen en daarom spaart men zich de moeite.
Bij het vaststellen van het aandeel van de investeringskosten voor aftapvoorziening in de totale investeringskosten van een bedrijf komen nog andere moeilijkheden om de hoek kijken. Dit aandeel kan op allerlei verschillende manieren worden geïnterpreteerd. Over welke tijdsperiode gaat het bijvoorbeeld (bij de introductie van een nieuwe techniek is het initieel aandeel vaak hoog, in de daarop volgende jaren zijn er daarentegen wellicht wel grote vervolginvesteringen in de opschaling van de dienst maar behoeft het aftappen weer minder investeringen). En betreft het een aandeel van de totale bedrijfsinvesteringen, of alleen die in telecommunicatie-infrastructuur? En wordt er onderscheid gemaakt tussen de verschillende infrastructuren en diensten, of wordt alles bij elkaar geteld? Al deze punten hebben een grote invloed op het uiteindelijke percentage van de aftapkosten ten opzichte van de gehele investeringskosten.

Kader 5.1. Meetbaarheid van investeringen voor aftappen

Eenmalige tegemoetkoming
In 1996 werd een tegemoetkoming voorzien van 2,9 miljoen gulden om reeds bestaande systemen aftapbaar te maken, bij wijze van overgangsregeling. Geen van de aanbieders zei zich te kunnen herinneren iets ontvangen te hebben, en ook de destijds grootste aanbieder KPN kon geen tegemoetkoming terugvinden. De behoeftestellers gaven aan dat voor de meeste van de in 1996 genoemde systemen nooit een tegemoetkoming is betaald, omdat er geen beroep op de regeling is gedaan en omdat de desbetreffende systemen geleidelijk zijn uitgefaseerd en nooit aftapbaar zijn gemaakt; slechts voor enkele specifieke diensten, zoals TFTS, is een bescheiden tegemoetkoming betaald.

Conclusie over investeringskosten
Voor de vraag wie de investeringskosten voor aftapbaarheid moet dragen, zijn er twee hoofdargumenten. Het eerste is dat de 'verantwoordelijke betaalt'; er bestaat echter verschil van mening over de vraag wie de verantwoordelijke is: de aanbieder die aan een wettelijke plicht moet voldoen zoals er zovele kostbare verplichtingen zijn, of de overheid die verantwoordelijk is voor de opsporing en staatsveiligheid? Onzes inziens gaan vergelijkingen met andere wettelijke

plichten, zoals voor brandpreventie of ARBO, mank omdat die plichten niet alleen het algemeen belang maar ook het eigen belang van het bedrijf waarborgen; bij aftapbaarheid is het beoogde belang het kunnen uitoefenen van de opsporings- en nationaleveiligheidstaken van de overheid, en niet mede het eigen belang van het bedrijf. Daarom lijkt het ons dat het principiële argument van verantwoordelijkheid hier meer in de richting wijst van de overheid dan van het bedrijfsleven. Het tweede argument echter betreft de kostenbeheersing: degene die de investeringskosten draagt zal zorgen voor doelmatige en dus goedkopere oplossingen. Aanbieders wijzen daarbij op de doelmatigheid van tappen als geheel, waardoor de investeringskosten in samenhang moeten worden beoordeeld met de operationele kosten en de feitelijke inzet van het tappen; dat vraagt echter een omvangrijke en complexe beoordeling die moeilijk te maken valt (vgl. par. 8.1). Daarom kan op dit punt beter worden gekeken naar de doelmatigheid van het aftapbaar maken sec. De behoeftestellers hebben daarbij een zwaarwegend argument, namelijk dat zij geen inzicht hebben, en ook nooit afdoende kunnen krijgen, in de precieze kosten die een aanbieder moet maken om te voldoen aan de aftapbaarheidsplicht. Wanneer de overheid de investeringskosten draagt, bestaat altijd het risico dat de aanbieder kosten opvoert die geheel of ten dele zijn gemaakt voor het inbouwen van andere functionaliteiten. Dit is een steekhoudend, pragmatisch argument dat kan opwegen tegen het principiële argument van de 'verantwoordelijke betaalt'. Niettemin blijft wel staan dat voor sommige kleine aanbieders de investeringskosten relatief hoog uitpakken, en dat juist in die gevallen soms wel inzichtelijk gemaakt kan worden wat de investeringskosten zijn – denk aan de kosten van het lidmaatschap van de NBIP waarmee Internetaanbieders aan hun aftapbaarheidsplicht kunnen voldoen. Omdat het telecomlandschap radicaal is veranderd sinds medio jaren negentig, moet dan ook in elk geval de politieke keuze van destijds voor de kostenverdeling opnieuw worden gemaakt, hetzij door deze bewust te bevestigen als zijnde nog steeds adequaat, hetzij door deze, wellicht voor bepaalde categorieën, te herzien.

5.2. Operationele kosten

Halverwege dit onderzoek, op 31 maart 2005, verscheen de lang verwachte (of gevreesde) ministeriële regeling met de vergoedingstarieven, die in art. 13.6 TW is aangekondigd.[137] De vraaggesprekken met de aanbieders vonden voor die datum plaats, dat met de behoeftestellers erna.

Het ontbreken van een kostenregeling had voor aanbieders en behoeftestellers verschillende kanten. Uit de vraaggesprekken blijkt dat een grote verscheidenheid aan vergoedingen werden gehanteerd, variërend per aanbieder maar soms ook per behoeftesteller. Deze situatie bood aanbieders de gelegenheid om steeds te onderhandelen over de tarieven, waarbij soms opvallend hoge tarieven werden gehanteerd, en waarbij behoeftestellers zich verbaasden over de grote onderlinge verschillen tussen aanbieders: een bepaalde taak kostte bij de een 20 euro en bij een ander 185 euro. Sommige operators openden zelfs 0900-betaalnummers waarop ze door de behoeftestellers konden worden gebeld. De keerzijde voor aanbieders was dat er ook regelmatig spanningen ontstonden omdat behoeftestellers met een volgens aanbieders soms vervelende toonzetting de gehanteerde tarieven steeds weer ter discussie stelden en wezen op goedkopere tarieven bij de concurrent, waarbij de aanbieder dan weer moest uitleggen dat zijn bedrijf anders in elkaar zat of dat over het tarief gewoon jaarlijkse afspraken waren gemaakt met het Parket-Generaal. Daarbij zijn volgens diverse aanbieders ook de nodige facturen onbetaald gebleven (overigens niet alleen vanwege verschil van mening over de tarieven, maar ook omdat opdrachtgevende behoeftestellers niet zelf een tapbudget hadden en voor de aanbieder niet duidelijk was wie nu eigenlijk de rekening moest betalen).
In dat spanningsveld zijn wel pogingen gedaan om tot gezamenlijke tarieven te komen, maar de partijen zijn niet tot elkaar kunnen komen. Vele aanbieders spraken hun teleurstelling uit dat hun constructieve medewerking met een onderzoek van Deloitte & Touche[138] door de behoeftestellers volledig is genegeerd. De behoeftestellers daarentegen stellen dat de aanbieders eisten dat zij op voorhand zouden instemmen met het voorgestelde kostenmodel, waarbij drie kostensoorten werden gehanteerd (infrastructurele kosten, operationele kosten, en een tussencategorie van bedrijfsvoeringskosten om aftappen feitelijk te kunnen uitvoeren), terwijl de behoeftestellers de

[137] Regeling kosten aftappen en gegevensverstrekking, 30 maart 2005, *Stcrt.* 31 maart 2005, p. 16, inwerkingtreding 2 april 2005.
[138] Deloitte & Touche, *Rapportage onderzoek justitiële kosten telecommunicatie*, Voorburg, 2 december 2002.

derde categorie een onjuiste interpretatie van de wet vinden omdat art. 13.6 TW alleen de eerste twee categorieën kent. Daardoor hebben aanbieders het rapport zelf onbruikbaar gemaakt, stellen de behoeftestellers. Aanbieders vinden echter dat de administratiekosten uit 13.6 lid 2 niet alleen directe maar ook indirecte administratiekosten omvat.
Naast de discussie over kostensoorten, staat ook de kostendiversiteit ter discussie. Aanbieders benadrukken dat zij in alle soorten en maten bestaan en verschillende benaderingen hebben. Een grote telefonieaanbieder met een eigen veiligheidsafdeling die doorlopend met taps bezig is kent nu eenmaal een andere kostenopbouw dan een kleine Internetaanbieder die plotseling een keer een tap moet uitvoeren. Volgens de behoeftestellers valt er echter best te praten wanneer een aanbieder overtuigend uitlegt waarom de kosten bij hem hoger uitvallen, maar de argumentatie daartoe overtuigt in de praktijk de behoeftestellers meestal niet. Zij hebben dan ook de stellige indruk dat de afgelopen jaren te veel betaald is aan aftapvergoedingen, en geven aan dat sommige operators zelf wel eens hebben laten vallen dat aftappen een winstgevende activiteit is geweest. Die indruk werd ook geuit door enkele kleine aanbieders, die in vraaggesprekken het vermoeden uitten dat grote aanbieders via de operationele kostenvergoeding een deel van de investeringskosten terugverdienden, waar zij dat door hun kleine omvang niet konden. De grote aanbieders ontkenden echter stellig dat zij aan aftappen verdiend hebben, eerder het tegendeel. Al deze beweringen zullen gekleurd zijn door de stellingname in het debat, maar in alle uitspraken kan een kern van waarheid zitten – het hangt er immers maar net van af welke kostensoorten je beschouwt als behorende tot de werkelijke operationele kosten.

Aan dit doorlopende debat heeft de wetgever nu in elk geval voorlopig een einde gemaakt door in de bijlage Regeling kosten aftappen en gegevensverstrekking uitgebreid maar uitputtend de handelingen op te sommen die declarabel zijn, te vermeerderen met 5% andere kosten. De minister is van oordeel dat alleen directe meewerkkosten in aanmerking komen, mede vanwege ‘de ervaring dat de bijkomende kosten gering zijn omdat verreweg de meeste algemene kosten van aanbieders investeringskosten zijn’.[139] Daarbij worden voor deze directe kosten indicatieve tarieven genoemd. In de media was te lezen dat de aanbieders deze tarieven schrikbarend laag noemden,[140] een conclusie die niet helemaal ongerechtvaardigd lijkt waar de Regeling een uurtarief van €26.25 hanteert en de standaardhandelingen voor gegevensverstrekking en aftappen fixeert op een kwartier respectievelijk een half uur.[141] Aan de andere kant moet worden vastgesteld dat dit indicatieve tarieven zijn, en dat wanneer een aanbieder kan aantonen daadwerkelijk meer kosten te hebben moeten maken – bijvoorbeeld wanneer een kleine dienstaanbieder een gespecialiseerde technische consultant moet inhuren om een tap te plaatsen – de meerkosten kunnen worden vergoed.
De Regeling lijkt in elk geval te leiden tot een verzakelijking van de opstelling van aanbieders; de behoeftestellers zeiden in het vraaggesprek een andere opstelling van aanbieders te merken sinds 2 april jongstleden. Waar sommige aanbieders voorheen wel eens telefonisch gratis een gegeven verstrekten, vragen zij sinds 2 april standaard een schriftelijke lastgeving, zodat zij kunnen factureren.
De reacties van de aanbieders suggereren, in lijn met de eerder gestrande poging, dat de Regeling buiten hen om tot stand is gekomen en dat geen overleg vooraf heeft plaatsgevonden over de hoogte van de tarieven. Ook DGTP gaf in het vraaggesprek aan ongelukkig te zijn geweest met het eenzijdige proces van totstandkoming van de regeling. Deze eenzijdigheid zou zich uiteindelijk ook tegen de behoeftestellers kunnen keren wanneer de regeling de verhouding met – voorheen loyale – aanbieders zodanig op scherp stelt dat zij niet alleen zakelijker omgaan met de behoeftestellers maar ook, zoals enkele aanbieders in het vraaggesprek vóór bekendmaking van de regeling al aangaven, wellicht minder geneigd zullen zijn om samen naar technische oplossingen te zoeken voor aftapbaarheidsproblemen.

[139] Regeling kosten aftappen en gegevensverstrekking, 30 maart 2005, *Stcrt.* 31 maart 2005, p. 16, inwerkingtreding 2 april 2005.
[140] Zie bijvoorbeeld 'Brinkhorst biedt veel te lage vergoeding internettaps', *de Volkskrant* 25 maart 2005.
[141] Men vergelijke bijvoorbeeld het bedrag dat XS4ALL noemt als de gemiddelde vergoeding voor een tap: €1364, aldus <http://www.xs4all.nl/overxs4all/privacy/privacy_jaarverslag.html>, met de vergoeding uit de regeling: €13,13 voor het plaatsen, €13,13 voor het verlengen, en €13,13 voor het vervroegd afsluiten van een tap. Een tap van 6 maanden die normaal afloopt kost dan €78,78, waarbij dan nog een bedrag kan komen voor het oplossen van storingen à €26,25 per uur. Het verschil betekent dat XS4ALL voorheen grote winst maakte op een tap, of dat zij in de toekomst zwaar verlies zal lijden op een tap, of beide.

Concluderend kunnen we vaststellen dat het – te – lang geduurd voordat een Regeling onder art. 13.6 lid 3 TW duidelijkheid heeft geschapen over de vergoeding van operationele kosten. In de tussenliggende periode lijkt er haast sprake te zijn geweest van een wildwestmarkt van tariefafspraken die vanuit het oogpunt van rechtszekerheid en rechtsgelijkheid bepaald onwenselijk was. Dat er nu een Salomonsoordeel is geveld in de vorm van een Regeling met uniforme tarieven is in dat opzicht zonder meer positief. Wel kan een vraagteken worden geplaatst bij de neutraliteit – en daarmee ook de wijsheid – van de Salomon in dezen.

5.3. Conclusie

De wetgever heeft ervoor gekozen de *investeringskosten* voor het aftapbaar maken bij de aanbieders neer te leggen, met de inschatting dat dit maximaal 1% van de normale investeringskosten zou vergen. Hoewel de investeringskosten moeilijk te bepalen zijn, hebben de onderzoekers de indruk dat de benodigde investeringen voor nieuwe netwerken of diensten wel substantieel meer bedragen dan de door de wetgever genoemde 1%. Dat geldt zeker voor (de destijds nauwelijks voorziene) kleinere dienstaanbieders, omdat de systemen voor aftapbaarheid maar deels schaalbaar zijn en er altijd sprake is van een fors startbedrag. Bovendien zijn er ook voortdurende kosten voor het aftapbaar *houden* van telecommunicatie. Daarom is een heroverweging nodig van de toedeling van de investeringskosten aan aanbieders.
Pragmatisch gezien ligt het voor de hand de aanbieder de kosten te laten dragen, omdat de overheid soms weinig zicht kan krijgen op de precieze investeringen en daardoor het risico loopt dat aanbieders hun kosten majoreren. Vanuit het perspectief van kostenbeheersing is het huidige systeem dan ook te prefereren. Daartegenover staat dat voor sommige kleine aanbieders de investeringskosten relatief hoog uitpakken, en dat soms wel inzichtelijk gemaakt kan worden wat de investeringskosten zijn (zoals de kosten van het lidmaatschap van de NBIP waarmee Internetaanbieders aan hun aftapbaarheidsplicht kunnen voldoen).[142] Principieel horen de kosten voor het aftapbaar maken van telecommunicatie ook thuis bij de overheid; er is immers sprake van een algemeen belang dat, anders dan bijvoorbeeld bij brandpreventieplichten, niet samenloopt met een privaat belang van de aanbieders.
Omdat het telecomlandschap radicaal is veranderd sinds medio jaren negentig, moet dan ook in elk geval de politieke keuze van destijds voor de kostenverdeling opnieuw worden gemaakt, hetzij door deze beargumenteerd te bevestigen als zijnde nog steeds adequaat, hetzij door deze, wellicht voor bepaalde categorieën, te herzien.

Voor de *operationele* kosten geldt dat daarvoor de overheid een vergoeding biedt aan de aanbieders. Het heeft erg lang geduurd voordat een ministeriële regeling duidelijkheid heeft geschapen over welke kosten precies vergoed worden, waardoor een chaotische periode van uiteenlopende tariefafspraken en -onderhandelingen heeft bestaan. Hieraan is in april 2005 een eind gekomen met de Regeling kosten aftappen en gegevensverstrekking, waarin standaardtarieven zijn vastgesteld. Aantoonbare meerkosten boven de standaardtarieven kunnen worden vergoed; de toekomst zal moeten leren wat als aantoonbare meerkosten kunnen worden beschouwd. Het feit dat de regeling eenzijdig is getroffen nadat eerdere pogingen tussen aanbieders en behoeftestellers om tot gezamenlijke tarieven te komen waren gestrand, bergt een risico in zich voor aftapbaarheid, doordat de verstandhouding tussen aanbieders en behoeftestellers op scherp wordt gezet, en loyale aanbieders mogelijk minder bereidwillig worden om gezamenlijk naar technische oplossingen te zoeken voor aftapbaarheidsproblemen.

6. Overige onderwerpen

In dit hoofdstuk behandelen we tot slot een aantal ‘losse’ onderwerpen die, naast de hoofdonderwerpen (het uitgangspunt dat alles aftapbaar moet zijn, de meewerkplichten en de kostenverdeling), van belang zijn voor de evaluatie van hoofdstuk 13 TW. We behandelen hier eerst de bepalingen uit hoofdstuk 13 over beveiliging en geschillenbeslechting, vervolgens de handhaving en de technische kennis bij de overheid, en ten slotte de vraag of de aftapbaarheidswetgeving de innovatie belemmerd of de concurrentie verstoord heeft.

[142] Merk ook op dat de OPTA in veel compleze telecomzaken verondersteld wordt goed in staat te zijn kostenniveaus te bepalen.

6.1. Beveiliging

De beveiligingseis van art. 13.5 TW wordt door alle partijen belangrijk gevonden. De aanbieders hebben de beveiliging over het algemeen goed op orde. De meeste aanbieders gaven in de vraaggesprekken aan dat zij sowieso al aan beveiligingseisen voldoen omdat dit vanuit hun eigen bedrijfsbelang nodig is. Als enige kritiekpunt merkte de NLIP op dat het Besluit beveiliging gegevens aftapbaarheid telecommunicatie (dat overigens pas na de periode van de vraaggesprekken in werking is getreden) te specifieke eisen bevatte, omdat sommige aanbieders de beveiliging intern op een bepaalde manier al goed hebben geregeld maar die dan moeten inruilen voor een ander, maar niet beter, systeem.
Een ander probleem bij kleine aanbieders zijn de eisen voor functiescheiding uit het Besluit: deze zijn bij aanbieders met slechts enkele medewerkers praktisch gezien moeilijk uit te voeren. Zowel aanbieders als behoeftestellers gaan hier echter pragmatisch mee om en noemen het niet als wezenlijk knelpunt.
Wat wel een probleem is, dat in de meeste vraaggesprekken met aanbieders werd genoemd, is dat volgens aanbieders de justitiële behoeftestellers vaak de verkeerde personen in het bedrijf benaderen, in afwijking van de bestaande procedures. Het steekt hen dat de hoge norm die zij zelf hanteren voor beveiliging aan justitiekant niet altijd wordt nageleefd. Aanbieders stelden dat het regelmatig voorkomt dat verzoeken niet binnenkomen op de beveiligde fax maar op de algemene fax, of bij het belcentrum waar tijdelijke krachten werken, of bij de dochteronderneming in plaats van bij de veiligheidsafdeling van het moederbedrijf, in strijd met de gemaakte afspraken over wie de te benaderen vertrouwenspersonen binnen het bedrijf zijn.
De behoeftestellers herkennen zich echter niet in dat beeld. Zij stellen juist dat de verantwoordelijke personen bij de aanbieders lang niet altijd bereikbaar zijn en dat zij daarom, bijvoorbeeld in het weekeind, hun toevlucht moeten nemen tot het telefoonboek en algemene nummers.
Deze opmerkingen van aanbieders en behoeftestellers, die elkaar niet hoeven tegen te spreken en beide juist kunnen zijn, geven ons de indruk dat in de uitvoering van de beveiliging aan beide kanten wel iets te verbeteren valt, met name in het nauwer naleven van procedures voor wie benaderd moet en kan worden voor tapverzoeken. Met die kanttekening kan worden geconcludeerd dat de beveiliging over het algemeen adequaat gevonden wordt en verder geen knelpunten oplevert.

6.2. Geschillenbeslechting

Artikel 13.3 TW, dat een mogelijk biedt bij AMvB regels te stellen over geschillenbeslechting rond tapdoorgiftevoorzieningen, wordt door alle geïnterviewde partijen als marginaal gezien. Er is geen gebruik van gemaakt en er bestaat tot nu toe ook geen behoefte aan specifieke geschillenbeslechtingsregels op dit punt. Meer in zijn algemeenheid staat formele geschillenbeslechting ook niet hoog op de agenda: in de praktijk worden geschillen steeds in onderling overleg opgelost, al dan niet met de stok van handhaving achter de deur.

6.3. Handhaving

In de vraaggesprekken kwam de handhaving vaak als een cruciaal aandachtspunt naar voren. Het continue spanningsveld van steeds weer nieuwe partijen, netwerken en diensten die aftapbaar moeten worden gemaakt (zie hfd. 3) maakt effectieve handhaving noodzakelijk. Dat vinden niet alleen de behoeftestellers, maar ook de aanbieders in verband met het scheppen van gelijke marktkansen.
De handhaving is pas laat op gang gekomen: het Agentschap Telecom is in de loop van 2004 serieus met het toezicht aan de slag gegaan. Voor die tijd was er geen sprake van actieve handhaving en was er over het algemeen een coulant beleid tegenover marktpartijen die de wet niet naleefden. Het feit dat de handhaving nu actief ter hand is genomen, wordt door iedereen toegejuicht.
Daarbij moet wel worden aangetekend dat de handhaving nog in de kinderschoenen staat,[143] en er zijn zowel bij aanbieders als bij behoeftestellers twijfels over de capaciteit van AT om effectief te kunnen handhaven, gezien de relatief kleine omvang van de toezichthouder en de dynamische

[143] Eind 2004 was volgens het AT ongeveer een vijfde deel van de 350 Internetaanbieders gecontroleerd.

en complexe markt. Ook is het nog een open vraag of AT voldoende technische kennis in huis heeft om steeds te kunnen beoordelen of een aanbieder aan de wet voldoet.
Ondanks deze vragen bestaat er zowel bij aanbieders als bij behoeftestellers wel een positieve grondhouding tegenover het AT. Men hoopt dat het Agentschap voldoende toegerust zal blijken om effectieve handhaving te garanderen.
We kunnen concluderen dat het toezicht door AT wezenlijk is voor de effectiviteit van de aftapbaarheidswetgeving: het is een onmisbaar sluitstuk van de wetgeving. Het is raadzaam om het komende jaar nauwlettend in de gaten te houden of het agentschap voldoende capaciteit heeft, in omvang en technische expertise, om toezicht te houden op het gehele telecomlandschap, zodat zonodig tijdig extra geïnvesteerd kan worden om de handhaving op peil te brengen.

6.4. Technische kennis

Een punt dat niet direct gerelateerd is aan de aftapbaarheidswetgeving, maar dat wel van belang is voor de effectiviteit van de aftapbaarheid, is de technische kennis bij de overheid van de vernieuwingen in de telecommunicatie. Door enkele aanbieders werd opgemerkt dat de technische kennis binnen de overheid geconcentreerd is bij een erg kleine groep mensen. In de praktijk krijgen de aanbieders tapverzoeken van een veel bredere kring van personen bij de justitiële behoeftestellers, die door gebrek aan technische kennis de nodige fouten maken (vgl. par. 4.1) of mogelijkheden niet benutten om net aftapbaar gemaakte nieuwe telecommunicatiediensten af te tappen, omdat zij nog onbekend zijn met deze diensten of omdat zij onvoldoende technische kennis hebben om afgetapte gegevens van zo'n dienst te kunnen interpreteren. Het beeld van een technisch kennisniveau bij de uitvoerende opsporingsambtenaren dat in het algemeen laag is, strookt met andere bevindingen[144] en is volgens ons een argument om te investeren in technische expertise bij de uitvoerende behoeftestellers, zodat het aftapbaar maken van telecommunicatie optimaal benut kan worden.

6.5. Innovatie

Een vraag die betrokken moet worden bij de evaluatie van de aftapbaarheidswetgeving, is of deze merkbare gevolgen heeft gehad voor de innovatie in de telecommunicatiesector. Tijdens de interviews zijn door aanbieders slechts één of twee voorbeelden genoemd van diensten die uiteindelijk niet op de markt zijn gekomen omdat men er niet in slaagde deze aan de aftapverplichting te laten voldoen. Het ging daarbij echter om relatief 'kleine' diensten, veelal toegevoegdewaardediensten, waar geen grote commerciële verwachtingen van bestonden. Ook als we het globale dienstenaanbod in Nederland naast dat van andere Europese landen leggen, lijkt er geen reden te zijn aan te nemen dat de Nederlandse aftapverplichting heeft geleid tot een substantieel kleiner aanbod van telecommunicatienetwerken of -diensten. Tevens zijn er in het onderzoek geen buitenlandse diensten aan het licht gekomen die louter vanwege de aftapbaarheidsverplichting niet in Nederland beschikbaar zijn.

Wel is door meer dan de helft van de gesproken dienstenaanbieders aangegeven dat ze bij de introductie van veel nieuwe diensten de architectuur en technische invulling hiervan hebben moeten aanpassen om te voldoen aan de aftapbaarheidsplicht. Uit de voorbeelden die we met de aanbieders hebben doorgesproken is op te maken dat dit in diverse gevallen kan leiden tot een ontwerp dat vanuit technisch, kostentechnisch of beveiligingsperspectief suboptimaal is.[145] Dit kan in beperkte mate als innovatiebelemmerend worden gezien.
Aan de andere kant wees één geïnterviewde erop dat zoiets als een aftapverplichting marktpartijen juist ook innovatiever kan maken, omdat ze een prikkel ervaren om onder moeilijkere omstandigheden toch iets te verwezenlijken ("Hoe strenger het aftapbaarheidsbeleid, hoe meer innovatie bij de gebruikers"). En als kwinkslag maar met een serieuze ondertoon werd ook opgemerkt dat de verplichting in elk geval tot innovatie in aftapvoorzieningen heeft geleid.

[144] Vgl. bijvoorbeeld de visienota van de Beleidsadviesgroep Computercriminaliteit, *Op weg naar... digitaal rechercheren*, 1996, en W.Ph. Stol, Handhaven: eerst kiezen, dan doen. Technische beperkingen en mogelijkheden, Ministerie van Justitie 2004, <http://www.justitie.nl/Images/deelrapport3_binnenwerk_tcm74-39111.pdf>, p. 46.
[145] Bijvoorbeeld omdat gekozen moet worden voor een oplossing waarbij telecommunicatie centraal wordt doorgeleid in plaats van decentraal, of omdat het gebruik van netwerkinterne veligheidsvoorzieningen en encryptie achterwege moeten worden gelaten.

Bij enkele relatief nieuwe ontwikkelingen bestaat momenteel nog onduidelijkheid over de mate waarin de aftapverplichting de innovatie remt. Voorbeelden zijn initiatieven voor nieuwe locale netwerken voor particulieren zoals die in sommige Nederlandse gemeenten worden genomen. Partijen worstelen daar met de aftapverplichting, en het probleem wordt versterkt door de relatief kleine schaal van veel van deze initiatieven. Anderzijds is het denkbaar dat een aftapvoorziening zoals de NBIP die aanbiedt, ook in dit veld een goede oplossing kan bieden. Het huidige onderzoek biedt nog onvoldoende inzicht in deze specifieke problematiek, maar het is een belangrijk aandachtspunt in de nabije toekomst.

Al met al is onze conclusie dat innovatie slechts in beperkte mate geremd wordt door de aftapvoorziening. Wel is het verstandig de gevolgen voor de innovatie van de aftapverplichting bij nieuwe initiatieven goed in de gaten te houden.

6.6. Concurrentieverstoring

Een andere vraag waar tijdens het onderzoek aandacht aan is besteed, is in welke mate de aftapverplichting gevolgen heeft gehad voor de mededinging, en in het bijzonder of het tot verstoring van de mededinging heeft geleid.

Nationaal
Een bij het merendeel van de gesprekken geplaatste opmerking is dat ‘kleine’ diensten (en daarmee dus ook nieuw geïntroduceerde diensten) zwaarder worden geraakt. De verplichte voorzieningen maken daar een veel groter deel uit van de totale investeringen dan bij de massadiensten. Er zijn door diverse aanbieders voorbeelden genoemd waarbij de aftapvoorzieningen gedurende de eerste twee jaar waarin de dienst beschikbaar was meer dan 10% van de totale investeringskosten bedroegen.
Het min of meer universele gegeven dat kleine diensten zwaarder worden geraakt, heeft verschillende implicaties voor kleinere en grotere bedrijven. Kleine bedrijven kunnen de kosten niet (tijdelijk) afwentelen op andere, beter renderende diensten, noch kunnen ze gebruik maken van bepaalde *economies of scope* (het inzetten van technische voorzieningen die reeds voor het aftappen van mainstream-diensten worden gebruikt). Daarbij moet echter worden aangetekend dat de aftapverplichting in dit opzicht lijkt op veel andere aspecten waar kleinere ondernemingen bepaalde nadelen ondervinden ten opzichte van grotere bedrijven (schaalvoordelen, *economies of scope*) en waar juist weer andere specifieke voordelen van kleine bedrijven tegenover staan, zoals grotere flexibiliteit, minder gehinderd door bestaande belangen, groeipotentie en minder hiërarchie.
Kleine bedrijven kennen nog een ander, meer algemeen nadeel: een aantal voorzieningen die moet worden getroffen zijn niet goed schaalbaar omdat ze per definitie een minimumomvang hebben. Het gaat hier bijvoorbeeld om niet-technische voorzieningen zoals de opleiding van personeel, de inrichting van beveiligde ruimten en andere veiligheidsvoorzieningen. In de praktijk heeft dat tot nu toe echter niet tot merkbare concurrentieverstoring geleid, mede omdat tot recentelijk kleine bedrijven gemakkelijker ‘onder de radar’ konden blijven bij gebrek aan actief toezicht (zie paragraaf 6.3).

Samenvattend kan voor de Nederlandse context worden gesteld dat er enige mate van mededingingsverstoring optreedt, omdat kleine bedrijven ongunstiger uit zijn dan grote bedrijven. Maar dat effect is, zoals hierboven beschreven, in de praktijk tot nu toe niet zichtbaar geweest en kan in onze ogen niet als ontoelaatbare concurrentieverstoring worden benoemd.

Internationaal
Een lastiger vraag is of de aftapverplichting tot *internationale* concurrentieverstoring heeft geleid. De meeste Westerse landen, in elk geval de EU-lidstaten en de VS, kennen aftapbaarheidsverplichtingen, die alle in meer of mindere mate de kostenstructuur en daarmee de competitiviteit van de in de sector actieve bedrijven raken. Rechtsvergelijking maakte geen deel uit van dit onderzoek, zodat naar aanleiding van verschillen in wetgeving zelf geen conclusies zijn te trekken.[146]

[146] Vergelijk het in noot 5 genoemde rapport over de situatie in de G7-landen.

Door sommige (maar lang niet door alle) aanbieders werd opgemerkt dat de uiteenlopende wetgeving in de EU rond de kostenvergoeding voor het aftapbaar maken van de infrastructuur – gewezen werd op onder andere Oostenrijk[147] – op zich concurrentievervalsend werkt. Met de toenemende flexibiliteit om diensten vanuit het buitenland aan te bieden, zouden aanbieders ervoor kunnen kiezen te vluchten naar 'aftapparadijzen' met aantrekkelijker aftapwetgeving. Voorzover we hebben kunnen nagaan zijn er echter geen dienstenaanbieders uit Nederland vertrokken als gevolg van de aftapverplichting, en zijn er ook geen diensten om die reden opgeheven. Ook kan niet gesteld worden dat Nederland minder nieuwe aanbieders van infrastructuur of diensten kent.dan omringende landen.
Ook beklagen verschillende vanuit Nederland opererende dienstenaanbieders zich dat ze moeten concurreren tegen aanbieders die vanuit het buitenland opereren en niet dezelfde, kostbare voorzieningen hebben getroffen. Eén operator stelt dat ze niet kan concurreren met uit het buitenland aangeboden e-maildiensten met veel opslagruimte, juist vanwege de aftapverplichting. We constateren dat het gebruik van nieuwe diensten vanuit het buitenland toeneemt, met name die van gratis diensten van bijvoorbeeld grote bedrijven uit de VS, maar ook van talloze kleinere diensten. Wanneer de aanbieders hiervan nalaten de verplichte aftapvoorzieningen te treffen, omdat ze relatief ongrijpbaar zijn, zou dat tot concurrentieverstoring kunnen leiden. Echter, het gaat vaak om diensten aangeboden door grote ondernemingen, die (ook omwille van hun andere producten en diensten) al een Nederlandse entiteit hebben. Uit het gesprek met behoeftestellers blijkt dat met sommige buitenlandse aanbieders van gratis diensten die een Nederlandse 'inbedding' hebben, afspraken worden gemaakt over de aftapbaarheid. En buitenlandse dienstenaanbieders die *tegen betaling* diensten in Nederland willen aanbieden, zullen vaak een Nederlandse entiteit oprichten, ondermeer om een goede facturering mogelijk te maken, zodat zij rechtstreeks aanspreekbaar zijn over de aftapbaarheidsplicht. Al met al lijken de gemaakte opmerkingen over concurrentieverstoring daarom eerder van theoretische aard.

Concluderend kunnen we stellen dat er ook vanuit een internationaal perspectief geen aanwijzingen zijn gevonden voor een aantoonbare, substantiële verstoring van de mededinging.

6.7. Conclusie

Twee bijkomstige bepalingen uit hoofdstuk 13 TW, over beveiliging en geschillenbeslechting, bevatten geen knelpunten in beleid of wetgeving. *Beveiliging* wordt door alle partijen belangrijk gevonden en deze is over het algemeen ook goed op orde. De wettelijke regeling is adequaat, zij het dat kleine aanbieders minder uit de voeten kunnen met de vereisten voor functiescheiding. Wel kan worden opgemerkt dat in de uitvoering van de beveiliging aan beide kanten iets te verbeteren valt, met name in het nauwer naleven van procedures voor wie benaderd moet en kan worden voor tapverzoeken. De bepaling over *geschillenbeslechting* is marginaal (want beperkt tot technische specificaties voor overdracht van tapsignalen) en wordt in de praktijk niet gebruikt. Van de overige onderwerpen die met aftapbaarheid samenhangen, is *handhaving* verreweg het belangrijkste aandachtspunt. Het toezicht door het Agentschap Telecom is wezenlijk voor de effectiviteit van de aftapbaarheidswetgeving en een onmisbaar sluitstuk van de wetgeving. De handhaving, die pas sinds 2004 effectief ter hand genomen is, staat nog in de kinderschoenen. Het is daarom raadzaam om het komende jaar nauwlettend in de gaten te houden of het agentschap voldoende capaciteit heeft, in omvang en technische expertise, om toezicht te houden op het gehele telecomlandschap, zodat zonodig tijdig extra geïnvesteerd kan worden om de handhaving op peil te brengen.
In het onderzoek is tot slot nog onderzocht of de aftapbaarheidswetgeving de innovatie of concurrentie in de telecomsector heeft belemmerd. De *innovatie* wordt slechts in beperkte mate geremd door de aftapvoorziening; soms moet worden gekozen voor een ontwerp dat vanuit technisch, kostentechnisch of beveiligingsperspectief suboptimaal is, maar er is geen blijk van een wezenlijke beperking van de innovatie in Nederland. Niettemin is het verstandig de gevolgen voor de innovatie van de aftapverplichting bij nieuwe initiatieven goed in de gaten te blijven houden. Wat betreft *concurrentie* kan voor de Nederlandse context worden gesteld dat er enige mate van mededingingsverstoring optreedt, omdat kleine bedrijven bij de aftapbaarheidsplichten

[147] Op 27 februari 2003 oordeelde het Oostenrijkse Constitutionele Hof dat de bepaling die de investeringskosten voor aftapbaarheid bij de aanbieders legt (§ 89 lid 1 Telekommunikationsgesetz) wegens strijd met de Oostenrijkse Grondwet opgeheven moet worden. Verfassungsgerichtshof 27 Februar 2003, G 37/02-16 etc., beschikbaar op <http://www.epic.org/privacy/intl/austrian_ct_dec_022703.html>.

ongunstiger uit zijn dan grote bedrijven. Dat effect is echter in de praktijk tot nu toe niet zichtbaar geweest en kan in onze ogen niet als ontoelaatbare concurrentieverstoring worden benoemd. Ook vanuit een internationaal perspectief zijn er geen aanwijzingen gevonden voor een aantoonbare, substantiële verstoring van de mededinging.

Deel III. Toekomst: ontwikkelingen

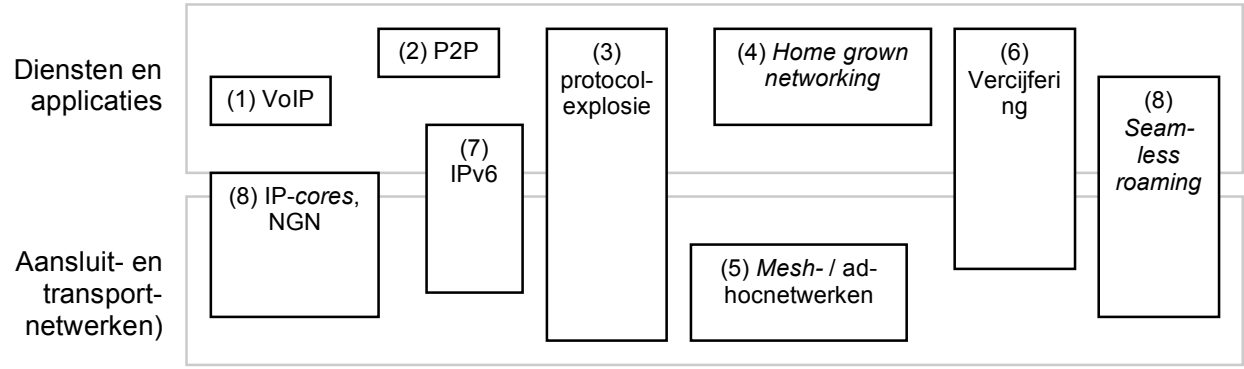
7. Ontwikkelingen in techniek, markt en identificatie

7.1. Technische ontwikkelingen

Er voltrekken zich momenteel talloze technische ontwikkelingen die mogelijk hun weerslag hebben op het aftapbaarheidsbeleid. Deze paragraaf beoogt een overzicht van recente en relevante ontwikkelingen te geven. Bij telecommunicatietechniek wordt vaak onderscheid gemaakt tussen het netwerkniveau (aansluitnetwerk, transportnetwerk) en het diensten- of applicatieniveau.[148] Omdat de hier te bespreken ontwikkelingen echter vaak ingrijpen op beide niveaus, is voor een meer thematische indeling gekozen.
We richten ons daarbij op ontwikkelingen die naar verwachting een direct effect op aftapbaarheid zullen hebben, met bijzondere aandacht voor de ontwikkelingen die door geïnterviewden als belangrijk werden beschouwd. Daarbij beperken we ons niet noodzakelijkerwijs tot wat er momenteel binnen de werking van hoofdstuk 13 Telecommunicatiewet valt; we nemen alle belangrijke ontwikkelingen mee die het doel van het aftapbeleid – het behoud van het instrument aftappen – raken.
De negen geselecteerde onderwerpen zijn:[149]

1. opkomst van Voice-over-IP (VoIP);
2. toename belang van peer-to-peer-toepassingen (p2p);
3. huidige protocolexplosie;
4. *home grown networking*;
5. *mesh networks* en ad-hocnetwerken;
6. vercijfering (encryptie);
7. invoer van het nieuwe Internetprotocol IPv6;
8. modernisering van basisnetwerken: IP-*cores* en NGN;
9. *seamless roaming* en andere vormen van intelligente routering;

De onderstaande figuur laat zien dat de genoemde onderwerpen het netwerk- en het diensten- en applicatieniveau raken, vaak op verschillende wijze. Zoals uit het volgende zal blijken, spelen deze nieuwe technische ontwikkelingen zich vooral in het Internetdomein af, en minder bij traditionele, circuitgeschakelde spraaktelefoniediensten.



7.1.1. De opkomst van Voice-over-IP (VoIP)

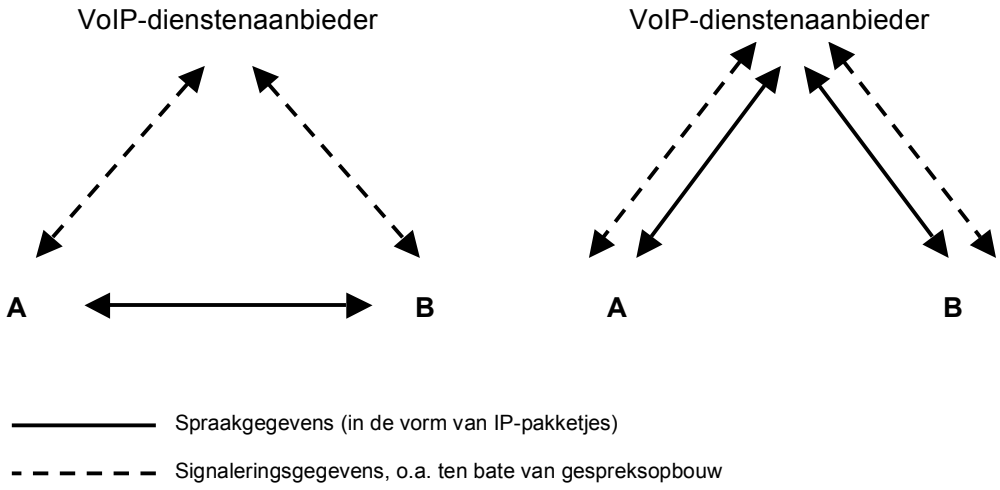
Eén van de meest in het oog springende ontwikkelingen is Voice-over-IP (VoIP). In bijna elk interview is deze techniek genoemd. Zoals de naam aangeeft, wordt bij VoIP telefoonverkeer via

[148] Naar believen kunnen er fijnere indelingen worden gemaakt, waarbij de keten in nog meer lagen wordt ontleed.
[149] Daarbij moet direct opgemerkt worden dat het capita selecta betreft uit een nog veel breder kader. Allerlei andere, voor aftapbaarheid meer perifere, onderwerpen, zoals satellietcommunicatie, *ambient networking* en *ubiquitous computing*, blijven buiten beschouwing.

het Internetprotocol afgehandeld (dus pakketgeschakeld) in plaats van via de traditionele circuitgeschakelde techniek. Dit belooft aanzienlijke kostenbesparingen. Deze liggen niet (alleen) in de techniek zelf, maar met name in de loskoppeling tussen transporteur en dienstenaanbieder die ze bewerkstelligen. VoIP werkt als een katalysator voor de huidige verschuivingen in de waardeketen (zie par. 7.2.4 over ontbundeling).
In de zakelijke wereld wordt VoIP vaak ingezet en het gebruik zet gestaag door. Uit recent onderzoek onder 300 middelgrote en grote ondernemingen blijkt dat 23% VoIP op een of andere manier toepast en dat 30% aangeeft dat de invoering of evaluatie van VoIP in de komende twaalf maanden gepland staat.[150] Hoewel het hier een Amerikaans onderzoek betreft, is dezelfde tendens in Europa en dus ook in Nederland waarneembaar. Ook in de consumentenwereld is VoIP aan een opmars bezig. De steeds grotere penetratie van kabel-Internet en ADSL maakt dat mogelijk. Er zijn overigens allerlei varianten van VoIP, afhankelijk van de plaats waar VoIP wordt ingezet in de keten (aansluitnetwerk, transportnetwerk, interne (bedrijfs)telefooncentrale). Ook zijn er diverse implementatievarianten, die al dan niet fabrikantspecifiek zijn.
VoIP-diensten worden aangeboden door specifieke dienstenaanbieders (bijvoorbeeld Rits Telecom uit Rotterdam en het Amerikaanse Vonage). Ook kabel- en ADSL-bedrijven brengen sinds kort Internettelefonie op de markt, waaronder UPC, Essent, CAI Westland, Zeelandnet, Casema, Wanadoo en Solcon. Daarnaast spelen de zogenoemde peer-to-peer-varianten (zie ook par. 7.1.2) van VoIP een bijzondere rol, zoals Skype. VoIP wordt nu vooral gebruikt via vaste netwerken. Echter, een brede adoptie van *flat fee* UMTS- en WiFi-hotspot-abonnementen zal dergelijke Internettelefoniediensten naar verwachting ook interessant kunnen maken voor mobiele gebruikers, omdat ze dan fors kunnen besparen op de kosten voor hun spraakverkeer. Inmiddels hebben diverse in Nederland actieve UMTS-aanbieders dergelijke *flat fee*-diensten geïntroduceerd. Vrijwel alle WiFi-hotspotdiensten hebben een *flat fee*-achtige structuur.[151] Hierbij kan gedacht worden aan de vele hotspots die KPN inmiddels aanbiedt, onder meer op de NS-stations.

Een problematisch punt bij VoIP is dat de dienstenaanbieder zelf het feitelijke gesprek vaak niet 'hoort langskomen' en dus niks kan registreren laat staan aftappen. Dat is weergegeven in Figuur 7.1 (linker schets). Een gespecialiseerde VoIP-dienstenaanbieder verwerkt wel het signaleringsverkeer dat benodigd is voor het opzetten van de verbinding. Vervolgens verloopt het spraakverkeer direct van de gebruikers A naar B en vice versa. Bij dat transport zijn weer allerlei andere partijen betrokken, zoals de exploitanten van de toegangsnetwerken van gebruikers A respectievelijk B en de Internet Service Provider (ISP) van A en B. Omdat de (Internet)verbinding van zowel partij A als partij B dus door andere partijen wordt geëxploiteerd dan de VoIP-aanbieder, is het voor laatstgenoemde in dit geval onmogelijk om zelf aan een tapplicht te voldoen. Dat zou alleen kunnen door specifieke (outsourcing-)afspraken te maken met alle mogelijke transporteurs/ISP's, maar dat kunnen er vele honderden zijn.
Figuur 7.1 (rechter afbeelding) schetst een situatie waarbij wel al het spraakverkeer via de VoIP-aanbieder verloopt. Dit scenario wordt onder meer door aanbieder Vonage in de VS gebruikt. Hoewel de aanbieder nu wel in staat is aan de tapverplichting te voldoen, is deze architectuur erg inefficiënt. (Er moet overigens wel op worden gewezen dat ook andere afwegingen dan de aftapplicht een rol kunnen spelen in de overweging om voor deze minder efficiënte routering te kiezen.)

[150] 'Wireless VoIP Gaining Traction in Business Market', persbericht In-stat, 8 februari 2005.
[151] Vaak rekent de klant hierbij af voor een tijdsblok van bijvoorbeeld één uur, en kan zij binnen die periode zonder beperkingen data uitwisselen.



Figuur 7.1: Routering van verkeer bij VoIP

Bij VoIP speelt verder het probleem dat behoeftestellers verwachten dat een tap op min of meer dezelfde wijze kan verlopen als een traditionele (PSTN-)telefonietap, maar dat is vaak niet het geval.[152] Hoewel het wel om een telefoniedienst gaat, zijn de gebruikte protocollen, methoden en achterliggende technieken volstrekt anders dan bij traditionele telefonie.
ETSI-NL, de norm die momenteel wordt toegepast voor aftapverkeer tussen aanbieder en behoeftesteller wordt gebruikt, gaat wel uit van de traditionele elementen waaruit het gewone analoge telefoonprotocol (PSTN) bestaat. Voor VoIP-protocollen, zoals het veelgebruikte SIP, kan echter niet zonder meer een equivalent gevonden worden gevonden voor de benodigde elementen.[153] (In technische termen: *mapping* van het SIP-protocol naar PSTN is niet eenduidig op te stellen. Met name omdat het twee qua opzet heel verschillende protocollen zijn, kent SIP allerlei *states* die geen tegenhanger in het PSTN-protocol hebben, en andersom.) Het gevolg daarvan is dat het huidige ETSI-NL-protocol in veel gevallen feitelijk ongeschikt is om ook Internettelefoonverkeer mee af te tappen.

7.1.2. Toename belang van peer-to-peer-toepassingen (p2p)

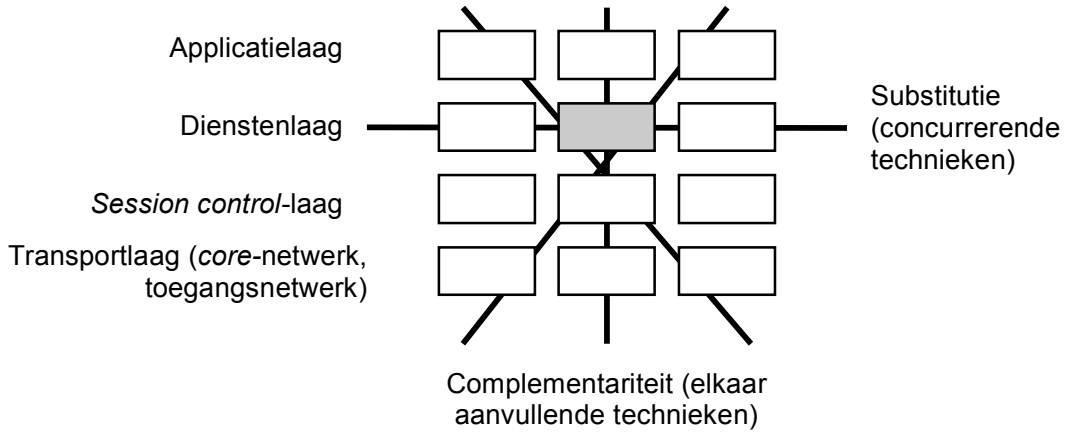
In het verleden was het vanzelfsprekend dat communicatiediensten gerealiseerd werden door bedrijven, en vervolgens tegen vergoeding op de markt aangeboden werden. Die vanzelfsprekendheid lag deels in het feit dat er meestal substantiële inspanningen en investeringen nodig waren om de dienst te 'bouwen'. In de laatste jaren beginnen echter de zogenoemde peer-to-peer-systemen (p2p) in populariteit sterk toe te nemen. In feite gaat het hier om systemen waarbij de eindgebruikers zelf diensten bouwen: ze voorzien zelf in alle benodigde functionaliteiten, en er is geen sprake meer van een dienstenaanbieder. Wel zijn er nog de partijen die het (reguliere) datatransport voor hun rekening nemen. Daarnaast is er sprake van een aanbieder van de benodigde (klant)software, maar deze partij kan moeilijk als een dienstenaanbieder worden aangemerkt.
De p2p-techniek verscheen het eerst op het toneel bij de – veelal illegale – uitwisseling van muziek en films. Marktopener Napster werd daarbij opgevolgd door KaZaA en eMule. Tegenwoordig worden steeds meer diensten in een p2p-vorm ontwikkeld. Het bekendste voorbeeld is Skype. In april 2005 gaf het bedrijf Skype aan dat het programma al bijna 100 miljoen maal was opgevraagd, en dat gebruikers van Skype in het eerste jaar al meer dan één miljard minuten met elkaar hebben gebeld. Er mag van worden uitgegaan dat het aantal regelmatige gebruikers in minder dan een jaar is gegroeid vanuit het niets tot enkele miljoenen. Ook allerlei berichtendiensten (*messenger*) kennen een p2p-techniek.

[152] Het is wel mogelijk wanneer bijvoorbeeld de VoIP-dienst via interconnectie aan een traditioneel PSTN-netwerk is gekoppeld. Dan kan wel gemakkelijker met gebruik van de huidige protocollen de communicatie afgetapt worden.
[153] Daar nog komt bij dat het genoemde SIP zeker niet het enige gebruikte protocol bij VoIP is, er is ook H323, MGCP, plus een keur aan leverancierssspecifieke protocollen waaronder dat van Skype.

Het meest in het oog lopende probleem bij p2p-communicatie is dat er geen dienstenaanbieder aan te wijzen is.[154] De taplast kan daarmee dus niet bij een dienstenaanbieder worden gelegd. Het alternatief, aftappen van het verkeer op de onderliggende transportnetwerken, is echter ook erg lastig. Gebruikers kunnen op allerlei verschillende plaatsen (en dus bij verschillende toegangsaanbieders) gebruik maken van hetzelfde p2p-account. Ook is het verkeer vaak lastig te interpreteren (zeker bij *proprietary* protocollen). Bovendien kan er sprake zijn van encryptie, en in dat geval hebben alleen eindgebruikers toegang tot de gebruikte sleutels. Onder meer bij Skype is sprake van een dergelijke encryptie.
P2p-technieken ontwikkelen zich ook steeds verder. In de meer geavanceerde varianten, zoals gebruikt door eMule, is er geen sprake meer van één bron en één bestemming; tientallen of honderden andere gebruikers kunnen ieder kleine porties van de gevraagde informatie versturen. Deze methode is met name ingegeven door de wens minder grijpbaar te worden voor handhaving van het auteursrecht (bij de illegale uitwisseling van muziek en films), maar sijpelt door naar allerlei andere (legale) toepassingen. Omdat er sprake is van veel bronnen is het minder eenvoudig de gegevensstroom af te tappen. Ook komen alle brokjes informatie in een – schijnbaar – willekeurige volgorde op de bestemming aan, wat het interpreteren van de informatie bemoeilijkt.

7.1.3. De huidige protocolexplosie

Er worden vrijwel dagelijks nieuwe communicatieprotocollen in gebruik genomen. Daarbij gaat het om nieuwe protocollen voor bestaande typen diensten, maar ook om totaal nieuw bedachte diensten. Ook de diversiteit aan apparatuur die via telefonie en Internet communiceert neemt snel toe. Naast de traditionele pc krijgen niet alleen apparaten als de Playstation en de Xbox een ethernetplug, maar straks ook allerlei andere, vaak huishoudelijke apparaten. Ook dat doet het aantal communicatieprotocollen dat in gebruik is snel toenemen. Er kan dus gesproken worden van een protocolexplosie. Daarbij gaat het zowel om een toename van protocollen die complementair aan elkaar zijn als om protocollen die met elkaar concurreren (dus substituten van elkaar vormen). Dat is in de onderstaande figuur grafisch weergegeven.[155] Steeds zal bij de introductie van nieuwe protocollen gekeken moeten worden in hoeverre bestaande *hand-over*-specificaties geschikt zijn om de tapgegevens over te dragen aan de behoeftestellers. Zeker bij totaal nieuwe type protocollen (zoals *instant messaging* dat was, enige tijd geleden) zal het nodig kunnen blijken een geheel nieuw overdrachtsprotocol te ontwikkelen.



Daarbij speelt ook het probleem van de veranderlijkheid van protocollen. In het verleden waren protocollen lange tijd stabiel, en de eventuele revisies die zo nu en dan werden aangebracht werden gedocumenteerd (*change management* / *change revision*). Tegenwoordig volgen veranderingen in protocollen elkaar, onder druk van de concurrentie, steeds sneller op. Ook zijn ze minder goed gedocumenteerd, en in het geval van leveranciersspecifieke protocollen soms

[154] We gaan hier voorbij aan de mogelijkheid dat de ontwikkelaar van de software zich tegelijkertijd ontpopt als aanbieder van (interconnectie)diensten, zoals bij Skype het geval is. In de laatste hoedanigheid kan deze natuurlijk wel als dienstenaanbieder wordt beschouwd.
[155] De figuur is afkomstig uit R.N.A. Bekkers (2005), *On the increasing importance of technical interoperability and ETSI's role in it. Discussion document ETSI/GA45(05)21, offered to the ETSI General Assembly on behalf of the Dutch members of ETSI*.

helemaal niet gedocumenteerd. Met name bij toepassingen die web-interfaces toepassen (denk aan webtoegang bij Microsoft Outlook, of aan Hotmail of Gmail) kan de interface heel regelmatig veranderen. Met name in die gevallen waarin wordt teruggevallen op het aftappen van het telecommunicatienetwerk (in plaats van de dienst) leidt dit tot problemen; bij elke protocolwijziging zal opnieuw gekeken moeten worden wat de structuur van de passerende gegevensstroom is en hoe daar de gewenste verkeers- en communicatiegegevens uit geabstraheerd kunnen worden.

7.1.4. *Home grown networking*

Gedeeltelijk in het verlengde van het bovenstaande over p2p-communicatie (par. 7.1.2) is er een heel scala van technieken in ontwikkeling waarbij eindgebruikers een steeds centralere rol spelen. Er is daarbij slechts een beperkte rol voor een (commerciële) dienstenaanbieder, en soms zelfs helemaal geen rol. Deze ontwikkeling speelt zowel op het dienstenniveau (waar het bovenstaande p2p een illustratie van is) als op het netwerkniveau. Een van deze technieken staat wel bekend onder de term *home grown networking*. Steeds meer kunnen eindgebruikers diensten gewoon thuis realiseren, bijvoorbeeld door het installeren van een e-mail-server of een hosting-server. Die hoeven ze dan niet meer – tegen vergoeding – van een bedrijf af te nemen. Nu gebeurt dat nog voornamelijk bij ervaren computergebruikers, maar naar verwachting zal dat in de nabije toekomst via standaardsoftware voor veel gebruikers een reële optie worden. Met het gemak waarmee een tegenwoordige gebruiker een persoonlijke thuispagina maakt, kan deze in de toekomst ook eigen e-mail-servers en dergelijke opzetten.
Het zal evident zijn dat bij een brede adoptie van *home grown networking* de effectiviteit en mogelijkheid om aftapverplichtingen op dienstenniveau op te leggen afneemt.

7.1.5. *Mesh networks* en ad-hocnetwerken

De traditionele visie is dat een communicatienetwerk een vaste, geplande vorm heeft en wordt aangelegd en beheerd door een netwerkexploitant. De netwerkstructuur is daarbij sterk centraal georganiseerd. Dit geldt voor zowel vaste als mobiele netwerken. Er is echter een tendens gaande waarbij netwerken steeds meer decentraal functioneren. Intelligentie schuift weg uit de kern; bij mobiele systemen krijgen de basisstations steeds meer intelligentie en autonomie. Dat kan problemen opleveren bij het realiseren van aftapvoorzieningen. Enkele recente voorbeelden daarvan werden in de vraaggesprekken genoemd bij hotspot-netwerken op basis van de WiFi-technologie. Daarbij bleek het realiseren van aftapvoorzieningen problematisch en duur te zijn.[156]
Nog veel lastigere vragen dringen zich op bij de introductie van netwerktechnieken en netwerktopologieën die bekend staan onder de namen *mesh networks* en ‘ad-hocnetwerken’. Dit zijn netwerken waarbij de terminals van de eindgebruikers zelf elementen (*nodes*) in het transportnetwerk vormen. De term *mesh networks* wordt meestal gebruikt als het vast opgestelde terminals betreft (bijvoorbeeld in woonhuizen); bij ad-hocnetwerken gaat het om mobiele terminals (en verandert het netwerk dus continu van vorm).
Dit type netwerken kan allerlei voordelen opleveren. Zo groeit de capaciteit vanzelf naarmate het aantal gebruikers toeneemt. Ook zijn minder gunstig gelegen gebruikers op een economische wijze te ontsluiten; een gebruiker hoeft namelijk niet altijd meer in het directe radiobereik van het basisstation te liggen. Beide type netwerken zijn zowel voor te stellen in een omgeving met een sterke rol voor een aanbieder als in een omgeving waar alleen nog maar eindgebruikers een rol spelen. De hier bedoelde technieken zijn ook opgepakt door grote leveranciers als Nokia (die zijn mesh-product ‘rooftop networks’ noemt), maar soms ook weer verlaten – mogelijk omdat het zich beter voor niet-commerciële dan voor commerciële toepassing leent. Toch verwachten technologie-experts in de toekomst veel van dergelijke technieken. Dat is des te meer het geval nu met IEEE 802.11-radiotechnologie (beter bekend onder de populaire naam WiFi), in combinatie met Linux, een betaalbare *mesh*-terminal worden gebouwd.

Het zal duidelijk zijn dat deze nieuwe netwerkconcepten consequenties hebben voor aftapbaarheid. Indien verkeer zich rechtstreeks tussen gebruikers kan afspelen, zullen er in feite bij elke *node* (terminal) aftapvoorzieningen moeten worden aangebracht. Hoewel het hier om *nodes* gaat die in eigendom kunnen zijn van de aanbieder, die op deze wijze in een mogelijk

[156] Centrale voorzieningen vragen om een totale (suboptimale) herziening van de hele verkeersstructuur in het netwerk, terwijl de installatie van talloze locale voorzieningen een heel kostbare aangelegenheid is.

opgelegde verplichting kan voorzien, is dit in veel opzichten een erg onaantrekkelijk scenario. Als er daarentegen wordt gekozen voor een opzet waarbij al het verkeer per definitie centraal wordt geschakeld (en zo relatief gemakkelijk voor aftappen zorg kan worden gedragen), dan worden echter alle eigenschappen te niet gedaan die *mesh*- en ad-hocnetwerken juist zo interessant maken.

7.1.6. Vercijfering (encryptie)

Het vraagstuk van de vercijfering van communicatie staat al lange tijd in de belangstelling. Er voltrekt zich echter een aantal ontwikkelingen die dit vraagstuk urgenter maken. We kunnen daarbij onderscheid maken tussen situaties waarbij de eindgebruiker bewust kiest voor het gebruik van encryptie en gevallen waarin die keuze niet bewust wordt gemaakt.
Bewuste encryptie wordt door eindgebruikers toegepast vanwege de vertrouwelijkheid van de gegevens, bijvoorbeeld om een communicatie aan de blik van echtgenoot, baas of justitie te onttrekken. De mogelijkheden hiertoe zijn steeds eenvoudiger. Veel e-mail-software beschikt over ingebouwde functies om berichten te versleutelen. Sterke vercijferprogramma's (zoals de Advanced Encryption Standard (AES) of triple-DES[157]) zijn goed toegankelijk en door velen te bedienen. Illustratief hierbij is de cryptofoon van Rop Gonggrijp. Het betreft hier een omgebouwd mobiel telefoontoestel dat in Nederland wordt aangeboden.[158] In antwoord op Kamervragen zei minister van Justitie Donner echter geen reden te zien dit toestel te verbieden.[159] Dit is overigens zeker niet het enige encryptieapparaat; al langer leveren partijen apparatuur voor sterk versleutelde verbindingen, onder andere op basis van producten van grotere leveranciers als Siemens.[160]
Met name *onbewuste encryptie* komt echter steeds vaker voor. De netwerkexploitant, de dienstenaanbieder of de gebruikte software schakelt daarbij encryptie in zonder dat de eindgebruiker daarom specifiek heeft gevraagd. Als de desbetreffende aanbieder ook over de sleutel beschikt, is er geen probleem. De taplast kan gewoon bij die partij worden neergelegd; de aanbieder moet vervolgens het verkeer zelf ontcijferen. Maar er zijn verschillende situaties waarin vercijfering wel tot problemen kan leiden. We schetsen er enkele.

- Er wordt een VPN-verbinding gebruikt. Dit is een afgesloten datanetwerk dat door één of meerdere bedrijven wordt gebruikt, dat onderliggend gebruik maakt van een publiek netwerk als het Internet. Een VPN komt tot stand middels het gebruik van *tunneling*-protocollen, zodat een veilige, afgeschermde verbinding kan worden opgebouwd. De eindgebruikers schakelen daarbij – vaak zonder dat ze zich daarvan bewust zijn – een sterke encryptie in. De voorzieningen daarvoor bevinden zich in elke Windows-computer en ook steeds vaker in routers voor thuisgebruik. Dergelijke VPN-verbindingen worden ook nu al veel ingezet, zeker in de bedrijfsmatige sfeer.
- Er vindt een brede uitrol van IPv6 plaats. Allerlei schakels in de communicatieketen, in binnen- en buitenland, schakelen encryptie in (zie par. 7.1.7 specifiek over IPv6).
- Er is sprake van encryptie en de dienstenaanbieder bevindt zich buiten de Nederlandse beïnvloedingssfeer.
- Er is sprake van encryptie maar er is geen sprake van een aanbieder. Dit komt momenteel onder meer voor bij het p2p-Internettelefonieverkeer van Skype.
- Encryptie wordt ingeschakeld door een aanbieder die niet als aanbieder van telecommunicatienetwerken of -diensten wordt gezien in de zin van de Telecommunicatiewet. Denk bijvoorbeeld aan webwinkels, waarbij gedurende het betalingsproces een veilige verbinding met HTTPS wordt ingeschakeld, maar ook aan allerlei andere Internetsites.

De eerste categorie bestond altijd al en zal ook blijven bestaan. Het betreft een klein aandeel van het totale communicatieverkeer. De wetgever heeft aangegeven dat het gebruik van cryptografie vrij is,[161] en dat is ook voor de toekomst een zinvol besluit omdat beperking van cryptografie nauwelijks zin heeft.[162] Een groeiende bedreiging zit evenwel in de tweede categorie: steeds

[157] Een vercijferingsalgoritme gebaseerd op DES (Data Encryption Standard) waarbij de informatie driemaal achter elkaar door hetzelfde algoritme wordt vercijferd.
[158] Zie <http://www.cryptophone.nl>.
[159] *Aanhangsel Handelingen II* 2003/04, nr. 891.
[160] 'Ophef over cryptofoon overdreven', *Emerce*, 20 november 2003.
[161] *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 10.
[162] B.J. Koops, *The Crypto Controversy. A Key Conflict in the Information Society*, diss. Tilburg, The Hague etc.: Kluwer Law International 1998.

meer verkeer zal zich aan de mogelijkheid tot aftappen kunnen gaan onttrekken, ondanks de huidige verplichting voor telecommunicatieaanbieders om door henzelf aangebrachte versleuteling ongedaan te maken.[163] Hoewel de schatting van experts uiteenlopen, kan het hierbij om tientallen procenten van het feitelijke communicatieverkeer gaan. Campagnes om de weerbaarheid van de burger te vergroten tegen Internetcriminaliteit en andere ongewenste digitale zaken (zoals spam en virussen) voeden voorts het gebruik van veilige – en daarmee soms lastig aftapbare – communicatie. Ook de steeds groeiende complexiteit van de markt (meer partijen, minder transparant) en de inherente zwakheden van radiocommunicatie nopen tot steeds betere en steeds regelmatigere bescherming.
Kort gesteld vormt vercijfering vanuit aftapperspectief een probleem wanneer:

- er geen sprake van een aanbieder is (bijvoorbeeld bij p2p-communicatie of randapparatuur);
- sleutels niet in handen zijn van een aanbieder (*end-to-end*-encryptie);
- sleutels in handen zijn van een andere aanbieder dan de partij die de taplast ontvangt;
- sleutels in handen zijn van een moeilijk aanspreekbare buitenlandse (diensten)aanbieder.

Overigens moet wel worden opgemerkt dat encryptie onderzoek van telecommunicatie zeker niet onmogelijk maakt. Verkeersgegevens zijn nog steeds beschikbaar, en ook is versleutelde inhoud niet zelden te kraken of blijken gebruikers slordig om te gaan met hun sleutels of wachtwoorden. Niettemin is encryptie volgens ons, mede vanwege bovengenoemde ontwikkelingen, wel een belangrijk aandachtspunt waar het gaat om het behoud van het middel aftappen.

7.1.7. De invoer van het nieuwe Internetprotocol IPv6

De brede invoering van IPv6 kan tot extra problemen leiden, maar dat hoeft niet altijd zo te zijn. In feite integreert IPv6 het veilige communicatieprotocol IPsec in de gehele infrastructuur. Alle apparaten zullen deze functionaliteit dus gaan ondersteunen. Dat betekent niet dat deze beveiliging vanzelfsprekend of 'automatisch' aanwezig is bij alle verkeer. Dat hangt af van de keuzen die de betrokken partijen maken; meerdere scenario's zijn denkbaar. Als de veilige modus echter wel wordt gebruikt, dan neemt de kans sterk toe dat het verkeer op het niveau van het toegangsnetwerk niet meer zinvol afgetapt kan worden. Vaak beschikken alleen dienstenaanbieders over de benodigde sleutels. Ook kan het zijn dat er sprake is van *end-to-end*-vercijfering, en in dit geval hebben alleen de twee eindgebruikers toegang tot de sleutel.
Overigens dient hier opgemerkt te worden dat de invoering van IPv6 nog steeds geen hoge vlucht neemt; bedrijven zien vooralsnog weinig noodzaak tot deze investeringen. Toch zal naar verwachting op langere termijn deze techniek het huidige protocol gaan aflossen.

7.1.8. Modernisering van basisnetwerken: IP-*cores* en NGN

Een belangrijke ontwikkeling is de 'Internetisering' van de zogenaamde *backbones*, de grote schakel- en transportnetwerken van telecommunicatieaanbieders. Daarbij wordt het IP-protocol de basis van alle technische systemen in het netwerk. Bij de nieuwste mobiele netwerken zoals UMTS is dat al grotendeels het geval, maar bij de al veel langer bestaande vaste netwerken minder.
Deze ontwikkeling is onder meer bekend onder de naam New Generation Networks (NGN). Vanuit verschillende hoeken wordt aan standaarden voor deze techniek gewerkt, waarbij er sprake is van een grote competitiestrijd tussen de desbetreffende organen (waaronder Europa's ETSI en de wereldwijde ITU). Natuurlijk spelen ook organen rondom Internet zelf, zoals de IETF, hier een grote rol.
De overgang naar deze nieuwe *cores* in de netwerken kan invloed hebben op aftapbaarheid en op de daarvoor benodigde investeringen. Door heel andere vormen van de routering van verkeer en heel andere adressystemen wordt het tappen complexer. De mate waarin op NGN gebaseerde systemen goed aftapbaar zullen zijn, zal mede afhangen van de hoek waaruit de techniek komt. Indien deze vooral uit de traditionele telecommunicatiewereld (zoals ETSI's TIPHON project) komt, dan zal er doorgaans bij het ontwerp al rekening zijn gehouden met aftapbaarheid. Dat is immers een van de uitgangspunten bij het ontwerp van een nieuwe techniek. Komen NGN-systemen echter vooral uit een andere hoek (ITU, en zeker bij IETF), dan is dat maar de vraag. Aftapbaarheid is in die gremia namelijk nooit een ontwerpuitgangspunt

[163] Art. 13 lid 1 TW jo. art. 2 sub e Besluit aftappen openbare telecommunicatienetwerken en -diensten.

geweest,[164] en het naderhand toevoegen van aftapmogelijkheden kan tot grote problemen en slechte compromissen leiden.

7.1.9. *Seamless roaming* en andere vormen van intelligente routering

Een andere ontwikkeling op netwerkgebied is *seamless roaming*. Hierbij wordt gedoeld op de situatie waarbij mobiele eindgebruikers ongemerkt kunnen wisselen van netwerk, zelfs tijdens een communicatiesessie.
Zo kan iemand een Internet-telefoniegesprek starten op kantoor, dat in eerste instantie via het WiFi-netwerk van het eigen bedrijf verloopt. Vervolgens loopt de persoon al bellende naar buiten en komt daarmee buiten het bereik van het eigen netwerk. Dan wordt de verbinding automatisch overgenomen door een UMTS-netwerk. Komt de persoon even laten buiten UMTS-dekking, dan wordt er overgegaan op GSM-GPRS-dekking. In weer een ander geval wordt naar een (goedkopere) *hotspot* omgeschakeld. Thuisgekomen verloopt de communicatie dan weer via het eigen draadloze netwerkje.
Een dergelijk scenario is in de toekomst zeer waarschijnlijk. Het heeft echter grote gevolgen voor de aftapbaarheid. Grofweg kunnen we twee situaties onderscheiden:

1. Er is sprake van een centrale partij die de regie voert in het proces. Dit is de (enige) partij waar de eindgebruiker een overeenkomst mee heeft. Deze partij laat delen van de communicatie via verschillende typen netwerken verlopen. Alle verkeer wordt echter door dezelfde aanbieder gerouteerd, en deze is dan ook technisch in staat om aan de aftapverplichting te voldoen. Overigens kan deze situatie wel nieuwe eisen stellen aan de overdracht van gegevens naar de behoeftestellers, zeker als de desbetreffende netwerken in technische zin sterk uiteenlopen.
2. De gebruiker zelf kiest uit allerlei verschillende netwerken en communicatiesystemen. Dat hoeft niet handmatig te gebeuren; een automatisch profiel kan kiezen voor het netwerk dat qua beschikbaarheid, tarieven, quality of service (QoS) en actuele netwerkbelasting het beste aan de wensen van de gebruiker voldoet. We duiden dit aan met de term *user-centered seamless roaming.* In dit kader wordt overigens ook wel de term *ambient networking* gebruikt. In dat geval kan het verkeer van een eindgebruiker sterk versnipperd zijn en moet een aftaplast naar vele partijen tegelijk om zicht op het totaal te houden.

Ook in de omgeving van vaste netwerken spelen ontwikkelingen die tot op zekere hoogte met *seamless roaming* te vergelijken zijn. Dat wordt meestal met de term *intelligente routering* aangeduid. Het gaat daarbij om apparaten die in opdracht van de gebruiker automatisch het aantrekkelijkste communicatienetwerk en/of de aantrekkelijkste aanbieder selecteert. Dat kan op basis van tarieven (gekoppeld aan bepaalde tijdstippen of bestemmingen), ondersteuning van bepaalde diensten, snelheid, *quality of service*-kenmerken (QoS), enzovoorts. Ook kan *load balancing* aan de orde zijn: het verdelen van capaciteit over meerdere verbindingen (ook tegelijkertijd). Dergelijke functies zullen steeds vaker in standaardapparatuur als routers worden ingebouwd, zonder dat de gebruiker daarmee onnodig wordt lastiggevallen.

7.2. Marktontwikkelingen

Veel marktontwikkelingen liggen in het verlengde van de mogelijkheden die nieuwe technologieën bieden, zoals het hierboven besproken VoIP en *home grown networking*. Deze aspecten zullen we hier niet herhalen. In deze paragraaf geven we meer algemene ontwikkelingen aan in de waardeketen en in de vraag naar telecommunicatiediensten.
Er is een selectie van zes onderwerpen gemaakt, te weten:

1. snelle adoptie van allerlei nieuwe vormen van diensten;
2. explosie van het verkeersvolume;
3. grotere diversiteit aan netwerken en technieken;
4. ontbundeling;
5. grensoverschrijdend (diensten)aanbod;
6. groeiende complexiteit van de waardeketen.

[164] Zie RFC 2804, May 2000, <http://www.ietf.org/rfc/rfc2804.txt>.

7.2.1. Snelle adoptie van allerlei nieuwe vormen van diensten

In de afgelopen jaren is het gebruik van nieuwe diensten en toepassingen snel toegenomen. Hier spreken cijfers voor zichzelf. Emerce berichtte in juni 2004 over de volgende cijfers:[165]

- er zijn 4 miljoen Nederlandse MSN-gebruikers;
- er vinden 22 miljoen MSN-gesprekken per dag plaats in Nederland;
- er zijn 60 miljoen *instant-messaging*-gebruikers in Europa;
- er zijn 100 miljoen sms-gebruikers in Europa;
- het aantal sms-berichten per dag in Nederland groeit naar verwachting van 4 miljard in 2003 naar 9 miljard in 2006.

Deze cijfers illustreren het aanzienlijke gebruik van betrekkelijk nieuwe diensten. Het gaat hier om communicatiestromen die niet verwaarloosd kunnen worden ten opzichte van reguliere spraaktelefonie.

7.2.2. Explosie van het verkeersvolume

De gemiddelde omvang van het verkeer per gebruiker neemt sterk toe. De alom bekende plaatjes van de groei van verkeer op de Amsterdam Internet Exchange is daar een mooie afspiegeling van.

In enkele jaren zijn veel Internetgebruikers via een 56 kbps-model doorgegroeid naar een kabel- of ADSL-abonnement van circa 500 of 1000 kbps. Veel aanbieders hebben pakketten aangekondigd waarin ook Internettelefonie en – soms – televisiedistributie in zijn opgenomen. Daartoe maken ze gebruik van ADSL(2)-verbindingen tot circa 20 Mbps. Een voorbeeld is Versatel, die recent een zeer snelle ADSL-dienst heeft geïntroduceerd waarover onder meer rechtstreekse voetbalwedstrijden worden verspreid. Met deze ontwikkeling zal de snelheid van een gemiddelde breedband-Internetverbinding naar verwachting snel toenemen.

7.2.3. Grotere diversiteit aan netwerken en technieken

Het aantal gebruikte telecommunicatietechnieken neemt snel toe. Dat geldt zowel voor het netwerkniveau als voor het toepassingen- en dienstenniveau. De adoptie van sommige daarvan verloopt met een fors tempo. Dat leidt tot een grotere spreiding in het gebruik van technieken. Zo kan voor de vaste telefoon thuis al gekozen worden uit de reguliere telefoonlijn, een kabeltelefoniedienst, ADSL/Internettelefonie, WLL of een lokaal WiFi-netwerk. In de toekomst komen daar weer allerlei technieken bij, zoals WiMax- en Fibre-to-the-Home- (FttH-)netwerken. Dergelijke voorbeelden zijn voor allerlei telecommunicatiemarkten te noemen. In lijn met wat is besproken in par. 7.1.3 kan dit leiden tot de vraag naar nieuwe overdrachtsspecificaties of varianten op bestaande overdrachtsspecificaties.

Steeds vaker gebruiken eindgebruikers meerdere gelijktijdige gegevensstromen. Een voorbeeld is de dienst die BySky in Nederland aanbiedt: het betreft hier een snelle Internetdienst die een ASTRA SES-satelliet voor de *downlink* gebruikt, en een telefoonlijn met modem voor de *uplink*. Andere voorbeelden van hybride systemen zijn de combinatie van DVB-T[166] en GSM. Het kan ook zo zijn dat eindgebruikers meerdere communicatiesystemen tegelijkertijd gebruiken voor een enkele communicatiesessie, zonder dat de aanbieders bij deze combinatie zijn betrokken – denk bijvoorbeeld aan videovergaderen en *instant messaging* tegelijkertijd, of aan gebruikers die via Skype aan het bellen zijn en tijdens het gesprek besluiten per e-mail of FTP bepaalde bestanden uit te wisselen. De verschillende toepassingen verlopen al dan niet via dezelfde dienstenaanbieders of via dezelfde netwerken.

Als het gaat om een hybride dienst die als een compleet geheel door een dienstenaanbieder wordt aangeboden, hoeft aftapbaarheid geen probleem te zijn (hoewel het wel om aanvullende uitwerking vraagt tussen behoeftestellers en aanbieders, onder andere wat het overdrachtsprotocol betreft). Maar daar waar eindgebruikers zelf diensten ‘samenstellen’, zal de behoeftesteller voor de uitdaging staan de verschilende gegevensstromen op een betekenisvolle wijze samen te brengen. Dat veronderstelt tevens dat de behoeftesteller alle relevante identiteiten van de betrokken gebruikers al vóór de communicatie in kaart heeft gebracht en de benodigde taplasten al heeft uitgevaardigd (zie ook par. 7.3).

[165] Beschikbaar op <http://weblog.roelonline.net/archives/001751.php>.
[166] DVB: Digital Video Broadcasting, een Europese standaard voor digitale televisie. DVB-T is de variant voor aardse zenders (terrestrial). Andere varianten zijn geënt op kabelnetwerken of satelliet.

7.2.4. Ontbundeling

Een van de belangrijkste ontwikkelingen in de telecommunicatiesector is de voortzettende ontbundeling ofwel ontvlechting. Decennia geleden waren diensten hard gekoppeld aan bepaalde netwerken, en daarmee aan bepaalde aanbieders. Die koppeling was zowel technisch als juridisch van aard. Nadat deze belemmeringen waren geslecht door voortschrijdende technische ontwikkelingen en door liberalisering van de markt, bleef de koppeling tussen netwerkexploitanten en diensten toch lange tijd relatief sterk. De nieuwe toetreders wisten vaak niet meer dan een fractie van de belangrijke markten voor onder meer telefonie en televisiedistributie te veroveren. Het behouden van deze dienstenmarkt wordt door dominante partijen ook als heel belangrijk gezien: de omzet van een telefoniedienst is – gerelateerd aan de transportinspanning – veel groter dan die van een 'platte' dienst die alleen bitjes vervoert.
Naar verwachting zullen hier op korte termijn grote veranderingen optreden. Veel experts verwachten dat de waardeketen over korte tijd volledig overhoop gegooid zal worden. De komst van VoIP en ADSL-telefonie zijn hierbij katalysatoren. Een vergelijkbare ontwikkeling zal zich ook bij mobiele telefonie voltrekken, indien *flat fee*-UMTS-diensten een breed publiek gaan bereiken. Deze ontwikkeling is ook waar te nemen bij Internetdiensten.
Steeds minder vaak kiezen eindgebruikers voor diensten als e-mail en *hosting* van hun eigen gebruiker. Er is een ruim aanbod van deze diensten door derde partijen, vaak ook gratis. Ook wordt er veelvuldig privé gebruik gemaakt van de dienstenfaciliteiten die de werkgever biedt. Dat voedt de introductie van de – goedkopere – kale toegangsdiensten, onder meer onder termen als *DSL direct*, *cable direct* en *white label* ISP-diensten.
De kern van deze ontwikkeling is dat er veel vaker een scheiding ontstaat tussen de dienstenaanbieder en de netwerkexploitant. Ook zal er, in toenemende mate, zelfs amper sprake zijn van enige relatie tussen deze partijen.
Overigens moet er ook melding van worden gemaakt dat tegelijkertijd zich een trend kan aftekenen waarbij eindgebruikers ervoor kiezen een bundel met verschillende diensten af te nemen bij dezelfde aanbieder (bijvoorbeeld telefonie, Internettoegang en televisiedistributie). Zowel gevestigde aanbieders als nieuwe toetreders hopen dat de klant gevoelig is voor dergelijke bundels, om de klant sterker te binden respectievelijk een klant over de streep te trekken om over te stappen.
Naar verwachting zullen beide tendensen (ontbundeling en bundeling) tegelijkertijd optreden en in zekere mate tot polarisatie leiden.

7.2.5. Grensoverschrijdend (diensten)aanbod

Samenhangend met de ontbundeling zullen netwerken en diensten steeds vaker geografisch gescheiden zijn en zullen ook in Nederland steeds meer diensten vanuit het buitenland worden aangeboden, zoals Hotmail, Gmail, MSN, allerlei *instant messengers* en Skype.

7.2.6. Groeiende complexiteit van de waardeketen: verschuivende rolpatronen

Het aantal verschillende rollen in de waardeketen neemt steeds verder toe. Was de rol vroeger beperkt tot die van transporteur en – eventueel – die van dienstenaanbieder, tegenwoordig valt een grote verscheidenheid aan rollen te onderkennen. Bij Internet hebben we onder meer te maken met de rollen voor Internettoegang (ISP), hosting, e-mail, chat, caching, *relaying*, doorsturen, enzovoorts. Ook bij netwerken en transport neemt het aantal rollen dat door verschillende partijen wordt ingevuld snel toe. Bij discussies over de invulling van Fibre-to-the-Home- (FttH)-netwerken worden er bijvoorbeeld talloze rollen onderscheiden, die vaak bij verschillende partijen worden ondergebracht.
Het toenemende aantal rollen leidt tot rolverschuivingen. Opmerkelijk is ook de al eerder genoemde tendens dat bepaalde rollen naar het eindgebruikerdomein verschuiven (peer-to-peer, *home grown networking*). De dynamiek in de waardeketen leidt soms ook weer juist tot rolvervaging. Ook de snel opkomende (burger)initiatieven voor besloten netwerken spelen hier een rol. Vele daarvan maken gebruik van draadloze technieken (zoals Wireless Leiden, dat WiFi gebruikt); daarnaast zijn er talloze lokale glasvezelinitiatieven. In de VS komen daarvoor de termen *wireless freenets* en *community networks* in zwang.
Deze ontwikkelingen leveren vragen op over degene op wie de aftapverplichting rust en hoe van de verplichting zo doelmatig mogelijk gebruik gemaakt kan worden ('bij wie klop ik aan?').

7.3. Ontwikkelingen in identificatie

Het koppelen van een persoon aan een eenduidige identiteit wordt in het Internettijdperk steeds lastiger. Toen telecommunicatie nog alleen uit reguliere telefoniediensten bestond, was er sprake van een eenvoudige en duurzame relatie tussen een nummer en een persoon. Alleen in uitzonderlijke gevallen lag de relatie wat ingewikkelder.[167]
Met de introductie van Internet is men personen gaan koppelen aan IP-nummers en – soms – e-mailadressen. Dit levert een aantal problemen op. Zo kan het IP-nummer waar een persoon gebruik van maakt regelmatig veranderen; bij dynamische toekenning gebeurt dat zelfs bij elke sessie, mogelijk meermaals per dag. E-mailadressen zijn gemakkelijk te veranderen, ook door de gebruiker zelf. Bij de reguliere e-mailsystemen (die van het SMTP-protocol gebruik maken) kan de gebruiker zelfs per verstuurd bericht zelf de in het bericht opgenomen identiteit intypen, zonder dat de netwerkbeheerder daar enig zicht op heeft.
In de nabije toekomst zal de relatie tussen personen en nummers nog veel gecompliceerder worden. We noemen enkele redenen.

- Gebruikers hebben meerdere IP-nummers. IPv6 ondersteunt tientallen tot zelfs honderden of duizenden nummers per gebruiker. Die zijn bedoeld om aan allerlei randapparaten, diensten en toepassingen te kunnen koppelen, tot zelfs de koelkast toe.
- *IP address tunneling* maakt IP-nummers veel minder goed zichtbaar.[168]
- Andere identiteiten dan het IP-nummer zullen naar verwachting steeds verder aan belang winnen, en ten slotte zelfs het IP-nummer tamelijk willekeurig maken. We kennen dat nu al in de vorm van het e-mailadres. Gebruikers kunnen reeds nu vanaf allerlei verschillende IP-nummers, bijvoorbeeld op verschillende locaties, dezelfde e-mail uitlezen. Er komen nog veel meer van dergelijke identiteiten en aliassen aan, zoals de 'Skype name', de MSN-identiteit, enzovoorts. Is de gebruiker thuis, dan activeert deze daar zijn Skype-account, dat doet de gebruiker ook op het werk, en in de nabije toekomst kan de klant het Skype-account ook activeren op de PDA of de GPRS- of UMTS-telefoon.
- Gebruikers nemen IP-toegang van steeds meer dienstenaanbieders en organisaties aan, al dan niet via dezelfde fysieke infrastructuur. Dat speelt ook al binnen een woning.
- Intelligente routers zullen steeds vaker op basis van bepaalde wensen van de klant (prijs, snelheid, kwaliteit, mogelijkheden) verschillende netwerkverbindingen activeren. Dat kan in de woning, maar ook goed in de mobiele omgeving: een mobiel apparaat kiest automatisch de aantrekkelijkste verbinding via residentieel basisstation (WiFi), hotspot (WiFi), bedrijfsnetwerk (WiFi), UMTS, GPRS of GSM.

Kort samengevat zal de betekenis van een IP-nummer als enkele, unieke verwijzing naar een eindgebruiker verdwijnen. IP-diensten komen steeds meer los te staan van de identiteit van de gebruiker; deze kan zijn identiteit eindeloos veranderen zonder een spoor achter te laten.

Een reële schets van een intensieve Internetgebruiker die illustreert dat de relatie tussen gebruiker en IP-nummer nu reeds een complexe aangelegenheid is

Het standaard Internetverkeer van onze gebruiker loopt via een ADSL-verbinding, meestal met het door de ISP toegewezen IP-nummer. Voor het thuiswerken wordt een VPN geopend en krijgt onze gebruiker een nieuw IP-nummer. Indien de ADSL-verbinding onverhoopt uitvalt, dan legt de router volautomatisch via ISDN een andere verbinding aan (wellicht via een andere provider), vanzelfsprekend met een ander IP-adres. Om on-line een document binnen te halen, wordt een inbelverbinding geopend naar de universiteit waar onze persoon werkt. Er wordt dan een IP-nummer toegewezen in het bereik van de universiteit, wat het mogelijk maakt toegang te krijgen tot ScienceDirect.
Al werkende wordt er nog even wat opgezocht via de mobiele telefoon. Via i-Mode worden enkele treintijden opgezocht (met weer een nieuw IP-nummer), en er wordt wat mail beantwoord die binnengekomen is op de PDA of de BlackBerry (ook weer met een nieuw IP-nummer).

[167] Denk hierbij aan telefooncellen, bedrijfstelefooncentrales en – later – belhuizen.
[168] Bij 'tunneling' wordt een gegevensstroom in een nieuwe omhulsel gesloten, een soort nieuwe enveloppe. Soms worden meerdere gegevensstromen in één nieuwe tunnel ondergebracht. Deze tunnel heeft een andere identiteit dan de oorspronkelijke datastroom. De oorspronkelijke verkeersgegeven zitten nu 'in de enveloppe', zijn feitelijk deel van de *inhoud* van het (nieuwe) bericht geworden en zodoende minder goed zichtbaar.

In deze schets zien we een gebruiker in korte tijd van zes verschillende IP-nummers gebruik maken. Deze schets kan naar believen in allerlei vormen worden uitgebreid: de *hotspot*, een antwoord tijdens een interactieve sessie op tv, enzovoorts.

7.4. Conclusie

De geschetste ontwikkelingen grijpen alle in meer of mindere mate en op verschillende wijze in op de aftapbaarheid van telecommunicatie. Deze ontwikkelingen kunnen worden samengevat aan de hand van enkele kernaspecten van het aftapbaarheidsbeleid.

Afbakening van de aftapplicht
Het uitgangspunt dat **alle openbare telecommunicatienetwerken en -diensten afluisterbaar moeten zijn** wordt onder druk gezet door de volgende ontwikkelingen:

opkomst van Voice-over-IP (VoIP)	De verkeersstroom loopt niet noodzakelijk langs de dienstenaanbieder.
toenemende belang van *peer-to-peer*-toepassingen (p2p)	Er is geen sprake van een dienstenaanbieder terwijl het verkeer om diverse redenen niet goed op netwerkniveau kan worden getapt.
home grown networking	
seamless roaming en andere vormen van intelligente routering	Communicatiegedrag valt steeds minder onder één domein; berichten en zelfs fragmenten van berichten raken verspreid over verschillende technieken en aanbieders. Dat maakt het plaatsen van een effectieve tap lastig; vooral de situatie waarbij er sprake is van *user-centred seamless roaming* is problematisch.

Doeltreffendheid
De **doeltreffendheid van aftappen** wordt onder druk gezet door de volgende ontwikkelingen:

toenemende belang van *peer-to-peer*-toepassingen (p2p)	Aftappen blijft mogelijk op netwerkniveau maar levert om diverse redenen (waaronder encryptie) geen zinvolle informatie op.
home grown networking	
huidige protocolexplosie	Nieuwe of sterk gewijzigde protocollen kunnen vragen om nieuwe of aangepaste overdrachtsprotocollen, hetgeen tot kosten en vertragingen leidt. Ook stelt de veranderlijkheid van protocollen uitdagingen aan het tappen van communicatie wanneer netwerken (in plaats van diensten) worden getapt.
mesh networks en ad-hocnetwerken	Daar waar deze structuren buiten het reguliere aanbiedersdomein vallen, onttrekt het verkeer daarop zich aan aftapmogelijkheden. Wanneer ze wel binnen dit domein vallen, dan stellen ze uitdagingen om aftapbaarheid op een gepaste wijze te implementeren.
vercijfering (encryptie)	Steeds meer verkeer onttrekt zich aan de mogelijkheid om betekenisvol geïnterpreteerd te worden: 1. als de eindgebruiker dat nastreeft, is verkeer technisch onleesbaar te maken; 2. steeds meer verkeer wordt standaard vercijferd verstuurd; lang niet altijd kan dat verkeer ontcijferd worden door een aanspreekbare aanbieder.
invoer van het nieuwe Internetprotocol IPv6	Idem.
seamless roaming en andere vormen van	Het wordt steeds moeilijk een volledig of

intelligente routering	voldoende volledig beeld te vormen van het communicatiegedrag van een eindgebruiker.

Doelmatigheid
De **doelmatigheid van aftappen** wordt onder druk gezet door de volgende ontwikkelingen:

huidige protocolexplosie	Door de steeds snellere opeenvolging van protocollen nemen de kosten om de aftapvoorziening te realiseren sterk toe.
opkomst van Voice-over-IP (VoIP)	Om geheel te voldoen aan de aftapplicht is het vaak nodig een suboptimale technische architectuur te kiezen, leidend tot hogere kosten.
mesh networks en ad-hocnetwerken	Om geheel te voldoen aan de aftapplicht is het vaak nodig een suboptimale technische architectuur te kiezen (tot zelfs aftapvoorzieningen op elke individuele terminal), leidend tot hogere kosten.
home grown networking	Om toepassingen die naar het privédomein zijn verschoven toch betekenisvol af te kunnen tappen, is veel meer inspanning vereist, en stijgen de daarmee gemoeide kosten.
seamless roaming en andere vormen van intelligente routering	De benodigde activiteiten om een voldoende compleet zicht te krijgen op alle communicatiestromen van een gebruiker nemen in omvang fors toe, en daarmee ook de kosten.
vercijfering (encryptie)	Steeds meer verkeer verschuift naar het vercijferde domein. Zowel in de situaties waar sleutels wel als waarin deze niet voorhanden zijn, stijgen daarmee de benodigde inspanning en de kosten.

Bij al deze ontwikkelingen stijgen de kosten, zowel voor aanbieders als voor behoeftestellers, en neemt daarmee de doelmatigheid af.
Daarnaast kan opgemerkt worden dat allerlei nieuwe ontwikkelingen om een steeds sterkere kennisbasis vragen bij alle betrokken partijen, ook bij de regelgever en de behoeftestellers. Bij *state-of-the-art*-technieken is ook kennis op het allerhoogste niveau nodig, zowel voor beleidsimplementatie (ontwerp van aftapspecificaties) als in de operationele zin. Dit vraagt om een aanzienlijke kennisontwikkeling en capaciteitsuitbouw, die ook gepaard gaat met extra kosten voor de overheid.

Aan de hand van het bovenstaande kan beargumenteerd worden dat de kosten om al het telecommunicatieverkeer in Nederland aftapbaar te houden zullen toenemen. Hoewel het in dit stadium onmogelijk is deze kosten exact in te schatten, is het aannemelijk dat het om een substantiële kostenverhoging gaat. De gehele doelmatigheid van het aftapinstrument als zodanig komt daarmee onder druk te staan.

Kostenverdeling
Uit de bespreking van de diverse technische en marktontwikkelingen moet de conclusie worden getrokken dat de kosten om netwerken aftapbaar te maken en te houden snel toenemen, vooral daar waar het allerlei nieuwe technologieën en diensten betreft. Op veel aspecten neemt de complexiteit toe en vragen ontwikkelingen om aangepaste dan wel nieuwe faciliteiten, al dan niet in combinatie met aangepaste of nieuwe overdrachtsprotocollen.
De ontwikkeling en adoptie van die nieuwe technologieën moet echter als onontkoombaar worden beschouwd, mede gezien de internationale en commerciële context waarin deze zich afspelen. In het verlengde hiervan kan ook de houdbaarheid van het uitgangspunt dat investeringskosten ten laste van de aanbieders komen, onder druk komen te staan.

Daarbij moet wel opgemerkt worden dat deze kostenstijging minder lijkt te spelen bij de bestaande diensten (traditionele vaste en mobiele telefonie). Juist bij nieuwe technologieën, diensten en toepassingen zijn de kosten echter disproportioneel groot. Dat speelt natuurlijk vooral bij nieuwe toetreders tot de markt, die immers vaak een nieuwe technologie als onderscheidende factor kiezen. Ook hebben deze kleinere partijen te kampen met hogere kosten door schaalnadelen en problemen met de (on)deelbaarheid van veel technische investeringen. Er moet echter op worden gewezen dat dit punt tevens speelt bij grote bedrijven: ook als deze bedrijven een nieuwe dienst of techniek introduceren, ondervinden zij voor die specifieke activiteit disproportioneel hoge kosten. Tijdens interviews zijn voorbeelden genoemd van situaties waarbij de aftapvoorzieningen bij dergelijke nieuwe diensten veel meer dan 1% van de totale investeringen vergden (zie par. 5.1). Het valt redelijkerwijs aan te nemen dat dergelijke situaties in de toekomst eerder vaker dan minder vaak zullen voorkomen.

Deel IV. Conclusies en aanbevelingen

Nu we beleid en wetgeving in kaart hebben gebracht (deel I), de uitwerking daarvan hebben besproken (deel II), en technische en marktontwikkelingen hebben verkend die het beleid en de wet nu en in de toekomst onder druk kunnen zetten (deel III), kunnen we de onderzoeksvragen beantwoorden ter evaluatie van het aftapbaarheidsbeleid.
Dit gebeurt in drie delen. We kijken eerst naar het verleden, waarbij niet het beleid zelf ter discussie staat, maar waarbij we evalueren of de vertaling van het beleid in wet- en regelgeving adequaat is geweest (par. 8.1). Vervolgens kijken we naar de toekomst, waarbij we het beleid en de wet- en regelgeving beoordelen op de houdbaarheid in het licht van huidige en te verwachten toekomstige ontwikkelingen (par. 8.2). Voor eventuele gesignaleerde knelpunten geven we tot slot in hoofdstuk 9 suggesties voor oplossingsrichtingen (par. 9.1). We eindigen met drie scenario's voor het beleid in de toekomst (par. 9.2) en een samenvattend overzicht van mogelijke oplossingsrichtingen (par. 9.3).

8. Evaluatie

8.1. Verleden

Onderzoeksvraag 1. Zijn de beleidsuitgangspunten uit 1996 voor aftapbaarheid adequaat vertaald in wet- en regelgeving?

De beleidsuitgangspunten uit 1996 zijn vertaald in hoofdstuk 13 van de Telecommunicatiewet, zoals die in 1998 in werking trad en sindsdien diverse malen is aangepast en aangevuld. Het antwoord op de eerste onderzoeksvraag, namelijk of deze vertaling adequaat is geweest, geven wij vanuit twee invalshoeken. In de eerste plaats kijken wij of de vertaling voldaan heeft aan de verwachtingen van de direct betrokken partijen, dat wil zeggen de behoeftestellers en de aanbieders; dit geeft een antwoord op de vraag vanuit het perspectief van de betrokken partijen. In de tweede plaats beoordelen wij of de vertaling van de uitgangspunten naar ons eigen inzicht – met inachtneming van de verwachtingen van de betrokken partijen – doeltreffend en doelmatig is geweest.

De beleidsuitgangspunten kunnen als volgt worden gegroepeerd:
a. Uitgangspunt: "openbare telecommunicatie is aftapbaar" (beleidsuitgangspunten 1, 2 en 3)
b. Meewerkplichten (beleidsuitgangspunten 3, 8 en 9)
c. Kosten en kostenverdeling (beleidsuitgangspunten 5, 6 en 7)
d. Overig (beleidsuitgangspunt 4, overige onderdelen van hfd. 13 TW)
Alle beleidsuitgangspunten, met uitzondering van nr. 7 over de eenmalige kostenvergoeding, zijn geïmplementeerd in hoofdstuk 13 van de Telecommunicatiewet en in onderliggende AMvB's en Ministeriële Regelingen. Heeft deze implementatie voldaan aan de verwachtingen van de direct betrokken partijen?
De *aanbieders* hebben weinig aan te merken op de vertaling van de uitgangspunten in de wet- en regelgeving. Zij hebben veelal meer kritiek op de inhoud van het beleid tot nu toe – die in deze evaluatie niet ter discussie staat – dan op de specifieke vormgeving ervan, en dan vooral op de kostenverdeling en de kostenvergoeding. De uitgangspunten dat zij voor aftapbaarheid moeten zorgen en dat zij moeten meewerken met behoeftestellers staan bij de aanbieders nauwelijks ter discussie: zij hebben zich, soms morrend, soms loyaal, geschikt in deze keuze van de wetgever. Wat de vormgeving van de wet- en regelgeving betreft valt bij sommige, vooral de kleine, aanbieders te beluisteren dat zij de besluiten en regelingen onnodig gedetailleerd vinden, terwijl andere, vooral de grote, aanbieders deze soms juist te algemeen en te weinig gedetailleerd vinden. In beide gevallen is er sprake van enige rechtsonzekerheid, maar dit wordt in de praktijk niet als een groot knelpunt ervaren, met uitzondering wellicht van de kleine Internetaanbieders; voor deze laatsten is echter een oplossing beschikbaar in de vorm van de verplaatsbare tapkast van het NBIP zodat zij zich niet in de details van de wetgeving hoeven te verdiepen.
De *behoeftestellers* vinden dat de uitgangspunten goed in wet- en regelgeving zijn vertaald: de wet is adequaat. De schoen wringt echter bij de naleving van de wet. Volgens de behoeftestellers zijn veel telecommunicatienetwerken en -diensten op het moment van introductie niet of niet

volledig aftapbaar; dat geldt niet alleen voor Internet, maar ook voor vaste en mobiele telefonie. Dat komt niet door gebreken in de wetgeving, maar door 'welwillende tegenwerking' van een meerderheid van de telecomaanbieders en door het feit dat handhaving pas laat – in de loop van 2004 – op gang is gekomen.

Wat kunnen wij als *onderzoekers* nu op basis van de bevindingen van het onderzoek en de verwachtingen van de betrokken partijen concluderen over de vertaling van de uitgangspunten in wet- en regelgeving? Wij kijken hierbij eerst naar de individuele beleidsuitgangspunten, en vervolgens naar het beleid als geheel. Dit laatste is nodig omdat de individuele vertaling grotendeels een vertaalslag betreft van elk onderdeel van het beleid naar een of meer wettelijke bepalingen. Of de implementatie van het beleid als geheel daarmee geslaagd is, betreft ook de vraag of de wet als geheel adequaat is. Adequaat kan in dit verband worden afgemeten aan de doeltreffendheid (effectiviteit) en de doelmatigheid (efficiëntie) van de wet: wordt het doel van het beleid, zoals vormgegeven in wet- en regelgeving, daadwerkelijk bereikt, en is de manier waarop dit doel wordt bereikt doelmatig?

De implementatie van de individuele uitgangspunten
De meeste individuele uitgangspunten zijn adequaat geïmplementeerd in wet- en regelgeving. De formuleringen van de wettelijke bepalingen zijn over het algemeen helder en leveren voldoende rechtszekerheid op, met uitzondering van de term 'openbaar'. Deze term is echter een rechtstreeks uitvloeisel van het tweede beleidsvoornemen, zodat dit knelpunt niet de vertaling van het beleidsuitgangspunt geldt maar de inhoud ervan; we komen hierop terug wanneer we de toekomstvastheid van de uitgangspunten beoordelen.
De mate van detaillering van de onderliggende regelgeving lijkt ons adequaat in het licht van het feit dat zowel grote als kleine aanbieders ermee uit de voeten moeten kunnen; de huidige besluiten en regelingen bewandelen een goede middenweg.

De implementatie van de uitgangspunten als geheel: doeltreffendheid
Hoewel de individuele uitgangspunten adequaat in wetgeving geïmplementeerd zijn, betekent dat niet per se dat het beleid als geheel ook adequaat is geïmplementeerd. Het doel van het beleid is 'het behoud van het middel aftappen van telecommunicatie',[169] dat wil zeggen dat telecommunicatie aftapbaar moet zijn zodat deze waar nodig afgetapt kan worden. Dit doel wordt in belangrijke mate maar niet volledig bereikt. Het overgrote deel van de openbare telecommunicatie is naar onze indruk uit de interviews wel aftapbaar, zij het niet altijd op de manier die voor de behoeftestellers het meest wenselijk is. Zij moeten dan hun toevlucht nemen tot suboptimale oplossingen, zoals netwerkverkeer tappen in plaats van een specifieke dienst. Daarnaast zijn er problemen met de aftapbaarheid bij de introductie van nieuwe netwerken of diensten op de markt: deze zijn veelal niet op dat moment aftapbaar, maar pas na verloop van tijd. Een derde knelpunt is dat de wetgeving – in navolging van het beleid – zich beperkt tot openbare telecommunicatie, terwijl belangrijke delen van de telecommunicatie, wellicht meer dan bij de beleidsvorming in de jaren negentig voorzien werd, wordt gevoerd over private netwerken of via private diensten. In deze drie opzichten is de effectiviteit van de wetgeving beperkt.
De verklaring van het eerste probleem ligt volgens ons ten dele in het feit dat de handhaving pas zeer laat op gang is gekomen, wellicht mede omdat de wet- en regelgeving onvoldoende instrumenten bevatte om vanaf het begin strakke naleving af te dwingen. Voor een ander deel moet de verklaring echter ook worden gezocht in de toenemende complexiteit en diversiteit van het telecomlandschap. De telecommunicatie ziet er niet meer zo uit als in 1998, en technische en marktontwikkelingen maken het illusoir dat 100% van alle telecommunicatienetwerken en -diensten altijd aftapbaar zijn (zie hfd. 7).
De verklaring voor het tweede probleem ligt voor een deel op hetzelfde vlak: de markt is te complex maar vooral ook te dynamisch om aftapbaarheid te kunnen verzekeren op het moment dat een nieuw netwerk of nieuwe dienst wordt geïntroduceerd. Hoewel het theoretisch is voor te stellen om aftapbaarheid in te bouwen en te testen vóór introductie, is dat in de praktische werkelijkheid onmogelijk. De telecommarkt is dynamisch en snel veranderend, waarbij doorlopend aanpassingen en vernieuwingen in de markt gezet worden. Het inbouwen en testen van aftapbaarheid vergt de nodige tijd – ten minste enkele maanden – waarbinnen niet alleen de

[169] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 7.

technische aftapbaarheid zelf moet worden ingebouwd maar waarin ook technische specificaties moeten worden ontwikkeld voor de overdracht van signalen naar de behoeftestellers. De innovatie en de internationale concurrentie in de telecomsector – die in het verleden niet geschaad zijn door de aftapbaarheidswetgeving – zouden volgens ons in de nabije toekomst wel serieus onder druk komen te staan wanneer de aftapbaarheid vóór introductie wel daadwerkelijk afgedwongen zou worden.
De verklaring voor het derde probleem, ten slotte, kan ook worden gezien in de ontwikkeling van een complexe en diverse telecommunicatiemarkt, waarbij grote gebruikersgroepen gebruik maken van in theoretisch opzicht besloten netwerken.
Door dit alles heen moet volgens ons echter ook een deel van de verklaring van niet-volledige aftapbaarheid worden gezocht in de niet-optimale verstandhouding tussen aanbieders en behoeftestellers. Deze verstandhouding is over het algemeen redelijk tot goed bij de traditionele aanbieders van telefonie, maar minder goed bij de nieuwe generaties aanbieders, waaronder de Internetaanbieders. Hoewel door de jaren heen wel stapje voor stapje iets meer vertrouwen is opgebouwd tussen behoeftestellers en nieuwe aanbieders, mede door brancheorganisaties als de NLIP, moet de onderlinge verstandhouding nog steeds als gespannen worden aangemerkt. Dit is niet verwonderlijk, gezien de grote cultuurverschillen die bestaan tussen politie en veiligheidsdiensten, met een sterk vertrouwen in de overheid en in orde en gezag, en de nieuwe generaties telecomaanbieders, die vaak wortels hebben in de jaren tachtig en negentig waarin zij het Internet beleefden als een vrije, soms anarchistische ruimte waar de overheid buiten moest blijven. Deze kloof lijkt nog versterkt te worden door een verschil dat regelmatig voorkomt in technische kennis tussen aanbieders van nieuwe telecommunicatie en individuele behoeftestellers, waardoor nogal eens misverstanden en spanningen ontstaan. Maar ook los van deze culturele kloof, bestaat er een inherent spanningsveld tussen de behoeftestellers met hun publieke belang van aftapbaarheid en de telecomaanbieders, ook de traditionele, met hun private bedrijfsbelangen. Dit spanningsveld is sinds 1998 niet wezenlijk veranderd en dreigt de laatste jaren eerder toe dan af te nemen. Dit biedt dan ook mede een belangrijke verklaring voor het feit dat een substantieel deel van de aanbieders, wellicht zelfs in aantal een meerderheid, niet spontaan geneigd is om aan aftapbaarheid te werken zolang er geen handhaving plaatsvindt (probleem 1) en voor het feit dat bijna alle aanbieders, ook de welwillende, telecommunicatie op de markt introduceren die nog niet aftapbaar is (probleem 2). Dit betekent dat om de doeltreffendheid van de aftapbaarheidswetgeving te vergroten, niet alleen werk moet worden gemaakt van effectieve handhaving, maar ook van het verbeteren van de verstandhouding tussen aanbieders en behoeftestellers.

Ondanks de gesignaleerde tekortkomingen in de aftapbaarheid, moet wel worden geconcludeerd dat de wetgeving in belangrijke mate effectief is geweest. Zoals gezegd is immers volgens ons het overgrote deel van de openbare telecommunicatie wel op enige wijze aftapbaar. Gezien de enorme ontwikkelingen in de telecommunicatiesector sinds de jaren negentig, is dat een belangrijk resultaat: het is sterk de vraag of zonder de wetgeving enige aftapbaarheid zou zijn overgebleven van de traditionele aftapbaarheid van de vaste PTT-telefonie, en bij gebrek aan prikkels zou bij nieuwe vormen van telecommunicatie zeker geen aftapbaarheid zijn ingebouwd. Qua effectiviteit kunnen het aftapbaarheidsbeleid en de -wetgeving dan ook als grotendeels succesvol worden gezien.

De implementatie van de uitgangspunten als geheel: doelmatigheid
Het tweede gedeelte van de beoordeling van de adequaatheid van de implementatie van het beleid valt lastiger te beantwoorden. Het antwoord op de vraag of de manier waarop het doel – aftapbaarheid – is bereikt, doelmatig is, hangt af van de beoordeling van de kosten en baten. Deze beoordeling kan niet goed op basis van dit onderzoek worden gedaan, omdat zowel de kosten als de baten omstreden zijn en er evenmin duidelijke criteria voorhanden zijn om een kosten-batenanalyse uit te voeren.
Wat de kosten betreft, kan worden geconstateerd dat deze vooral liggen in de financiële kosten van het aftapbaar maken en aftapbaar houden van de telecommunicatie. Het onderzoek geeft geen aanwijzingen dat er in de achter ons liggende jaren andere substantiële maatschappelijke kosten zijn ontstaan, zoals beperking van innovatie of van de mededinging. De exacte financiële kosten voor aftapbaarheid konden binnen het bestek van dit onderzoek niet gekwantificeerd worden; wel zijn er voldoende aanwijzingen dat de kosten zeker meer bedragen dan de 1% van

de investeringskosten die bij de behandeling van de Telecommunicatiewet als maximum ('meestal minder') werd genoemd en die een rol speelde bij de acceptatie van de regeling om investeringskosten bij aanbieders neer te leggen (zie par. 2.6.1). Met name voor kleine aanbieders zijn de aftapbaarheidskosten relatief hoog, omdat deze maar beperkt schaalbaar zijn. De baten zijn evenwel lastiger te vatten. De aanbieders bleken in de gesprekken deels te kijken naar de effectiviteit van tappen als zodanig – dus het concrete effect op de criminaliteitsbestrijding – wanneer hen gevraagd werd naar de baten van het beleid; een ander deel van de aanbieders beschouwde vooral het gebruik dat werd gemaakt van de aftapbaarheid – dus het aantal taps – als maatstaf voor de baten. Aan de hand van dit laatste criterium beoordeelden de meeste aanbieders de doelmatigheid van aftapbaarheid als redelijk tot goed bij vaste en GSM-telefonie, en als matig tot zeer slecht bij Internet en nieuwe generaties telefonie. De behoeftestellers daarentegen achten dit een verkeerde zienswijze, omdat niet het concrete gebruik maar de beschikbaarheid als baat moet worden gezien. Het feit zelf dat een vorm van telecommunicatie aftapbaar is, vormt het doel, niet het aantal taps dat wordt geplaatst of de effectiviteit daarvan. Ook de kleinste netwerken of diensten – waar vanwege de omvang weinig getapt zal worden – moeten aftapbaar zijn, omdat anders moedwillige misdadigers en terroristen juist die netwerken of diensten op zouden zoeken voor hun communicatiebehoefte. Daar komt bij dat, wat sommige aanbieders zelf ook opmerkten, niet kan worden gezegd dat veel taps per se meer baten opleveren dan weinig taps, omdat de oplossing van één belangrijke zaak door één tap al maatschappelijk voldoende waardevol kan zijn.
Dit laatste geeft tegelijk ook aan dat een kosten-batenanalyse nauwelijks te maken valt, omdat de financiële kosten en de maatschappelijke baten ongelijksoortig en daarmee incommensurabel zijn.
Een en ander betekent dat wij de doelmatigheid van het beleid niet kunnen beoordelen. Dat wil echter niet zeggen dat daarmee doelmatigheid geen aandachtspunt is. Waar de wetgever kosten oplegt aan private partijen – en indirect aan telecomgebruikende consumenten – zal op zijn minst de batenkant verantwoord moeten worden. Dit is niet alleen van belang voor de legitimiteit van de wetgeving, maar ook voor de effectiviteit ervan. Een van de oorzaken van de niet-optimale verstandhouding tussen behoeftestellers en aanbieders, en daarmee van de niet-optimale naleving van de wet, is volgens ons dat de baten van het beleid verschillend worden gewaardeerd door behoeftestellers en aanbieders. Zolang aanbieders kijken naar het concrete aantal taps dat wordt geplaatst of naar de effectiviteit van die taps als legitimatie voor de kosten die zij moeten maken, houden zij een onbevredigd gevoel wanneer zij nieuwe netwerken of diensten aftapbaar hebben gemaakt en het vervolgens lang duurt voordat zij, en dan nog mondjesmaat, taplasten krijgen. Zij zijn dan minder geneigd om de volgende dienst direct weer aftapbaar te maken, omdat zij veronderstellen dat de kosten daarvoor weggegooid geld zijn. Het is daarom van belang dat behoeftestellers en de wetgever aangeven wat het belang is van de aftapbaarheidswetgeving en wat de baten daarvan zijn. Indien de wetgever de visie van de behoeftestellers deelt, moet hij samen met de behoeftestellers de aanbieders ervan zien te overtuigen dat de enkele aftapbaarheid een belangrijk maatschappelijk nut heeft, ook zonder dat er concreet wordt getapt.[170] Een andere mogelijkheid is om, zoals de overheid van de Verenigde Staten sinds jaar en dag doet,[171] jaarlijks een overzicht te publiceren van het aantal justitiële taps

[170] Eerdere opmerkingen van die strekking door de wetgever bij de behandeling van de Telecommunicatiewet hebben veel aanbieders kennelijk niet overtuigd. Een betere argumentatie zal nodig zijn dan de volgende passage geeft: 'Kosten/baten-vragen lenen zich ten aanzien van het onderwerp bevoegd tappen niet goed voor een eenduidige of objectieve interpretatie. Het WODC heeft geconcludeerd, en de regering onderschrijft deze conclusie, dat de maatschappelijke opbrengsten van de telefoontap waardevol zijn. (...) Waar het derhalve om gaat is om met een goed geformuleerd en uitgevoerd aftapbeleid de waarde van de tap overeind te houden (...) zonder dat er gaten vallen. (...) De kosten/baten-analyses van de tap moeten derhalve in het hierboven weergegeven perspectief worden geplaatst. De vraag of de kosten die gepaard gaan met het aftapbaar maken van telecommunicatie nog wel in verhouding staan tot de informatie die wordt verkregen uit de tap is daarom hier niet aan de orde.' *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 132.

[171] De Administrative Office of the United States Courts publiceert jaarlijkse federale en statelijke tapstatistieken op <http://www.uscourts.gov/library/wiretap.html>. In 2004 waren er bijvoorbeeld 980 taps in de diverse staten en 730 federale taps. Bij de federale taps werden gemiddeld per tap 3266 communicaties onderschept, waarvan 651 belastend waren, tegen gemiddelde kosten van $75.000 per tap. 693 taps betroffen telefonie, 11 direct afluisteren ('oral interception'), 12 elektronische taps (semafoon, fax en computer) en 7 een combinatie. In deze tapzaken werden 2389 arrestaties verricht, leidend tot veroordeling van 186 personen. Deze cijfers zullen de komende jaren nog stijgen; vergelijk de cumulatieve tabel van arrestaties en veroordelingen voor tapzaken uit 1994-2004 op <http://www.uscourts.gov/wiretap04/Table9-04.pdf>. Let wel: deze cijfers moeten in de context van het Amerikaanse rechtssysteem worden gezien, waarin tappen een relatief gering belang heeft, en kunnen niet zo maar worden vergeleken met Nederland. Wij noemen de cijfers hier om aan te geven dat men in de VS deze cijfers kennelijk gewoon kan registreren en jaarlijks publiceren, iets wat de Nederlandse regering tot nu toe heeft afgewezen (de minister beschikt 'niet over landelijke gegevens van het aantal justitiële taps op jaarbasis. (...) Ik zie geen meerwaarde in een afzonderlijke landelijke registratie

en van het percentage van de tapzaken dat tot een veroordeling heeft geleid. Een adequate verantwoording van het nut van de aftapbaarheidswetgeving zal het draagvlak bij de aanbieders voor de wet vergroten en daarmee zal de wetgeving effectiever kunnen zijn.

Samenvattend kunnen we de eerste onderzoeksvraag als volgt beantwoorden. De beleidsuitgangspunten uit 1996 zijn elk adequaat vertaald in wet- en regelgeving. Het beleid als geheel is ook adequaat geïmplementeerd in wet- en regelgeving, aangezien de aftapbaarheid van openbare telecommunicatie grotendeels gerealiseerd is en aldus het doel van het beleid – het behoud van het middel aftappen – grotendeels bereikt wordt. De technische aftapbaarheid is echter niet volledig bereikt – en behoeftestellers noemen het niet-aftapbare deel ernstig – door enerzijds gebrekkige handhaving en een niet-optimale verstandhouding tussen behoeftestellers en aanbieders, en anderzijds de complexiteit en diversificatie in de telecommunicatiesector. Waar het eerste probleem – de handhaving en de onderlinge verstandhouding – zonder aanpassingen in het beleid aangepakt kan worden, is het de vraag of het tweede probleem – de ontwikkelingen in techniek en markt – de aftapbaarheid in de toekomst niet dusdanig blijvend onder druk zet dat een herziening van het tot dusverre grotendeels effectieve beleid aangewezen is. Dit vraagt om zelfstandige reflectie op de toekomst, die we in de volgende paragraaf als tweede deel van de evaluatie ondernemen.

8.2. Toekomst

Onderzoeksvraag 2: Zijn de beleidsuitgangspunten en de huidige wet- en regelgeving voor aftapbaarheid voldoende toegesneden op huidige en toekomstige ontwikkelingen in telecommunicatie? Dat wil zeggen: kan het huidige wettelijke kader adequaat invulling geven aan de behoefte tot aftappen van de behoeftestellers in het licht van de ontwikkelingen?

Het beleid en de daarop gebaseerde wetgeving zijn tot nu toe grotendeels effectief geweest; de doelmatigheid ervan valt moeilijk in absolute zin te beoordelen (par. 8.1). De vraag is of de effectiviteit in de toekomst ten minste even groot kan zijn, en of de doelmatigheid in relatieve zin ten minste niet zal afnemen. De ontwikkelingen in techniek en markt die wij signaleren (zie hfd. 7) veroorzaken diverse problemen die de doeltreffendheid en de doelmatigheid onder druk zetten. Dit geldt voor de eerste pijler van het aftapbeleid, de technische aftapbaarheid, in combinatie met de derde pijler, de kostenverdeling. De tweede pijler, de meewerkplichten bij concrete lastgevingen, is niet problematisch, omdat deze plichten niet of nauwelijks worden beïnvloed door de technische en marktontwikkelingen. In het navolgende concentreren we ons daarom op de technische aftapbaarheid en de kostenverdeling.
Volgens ons zijn het huidige beleid en de huidige wet- en regelgeving niet adequaat om in de toekomst aftapbaarheid te garanderen. Wij onderbouwen dit antwoord door de problemen te bespreken waar beleid en wetgeving tegenaan lopen, zowel problemen veroorzaakt door nieuwe ontwikkelingen als de reeds bestaande problemen die in de vorige paragraaf zijn geconstateerd. Deze problemen kunnen worden gegroepeerd in een vijftal probleemvelden, die we bespreken in volgorde van urgentie, van problemen die op korte termijn spelen tot problemen op iets langere termijn.
In deze paragraaf beperken wij ons overigens tot het signaleren van problemen en knelpunten; mogelijke oplossingen hiervoor komen in het volgende hoofdstuk aan de orde.

Probleemveld 1: handhaving, spontane naleving en de onderlinge verstandhouding tussen behoeftestellers en aanbieders
In de vorige paragraaf constateerden wij dat er in de afgelopen periode problemen optraden in de handhaving, dat de wet door een belangrijk deel – mogelijk een meerderheid – van de aanbieders niet spontaan werd nageleefd, en dat de onderlinge verstandhouding tussen

van de inzet van opsporingsmethoden', *Aanhangsel Kamerstukken II* 2002/03, nr. 1035; herhaald in nr. 1553 en in 2003/04, nr. 219). Overigens zijn er wel incidenteel cijfers bekendgemaakt: in 1999 werden 10.000 justitiële taps uitgevoerd, waarvan 3000 vast en 7000 mobiel (*Kamerstukken II* 2000/01, 27 591, nr. 2). De evaluatie van de wet BOB noemt een totaal aantal van 7500 tapbevelen in zeven (van de 25) regio's in 2003, met de constatering dat 'overal het aantal tapbevelen explosief gestegen [is] ten opzichte van het jaar 2000', A. Beijer e.a., *De Wet bijzondere opsporingsbevoegdheden – eindevaluatie*, WODC/Boom Juridische uitgevers 2004, <http://www.wodc.nl/images/B&O_222_alles_tcm11-15661.pdf>, p. 57; zie p. 147ff voor de context van dit indicatieve cijfer.

behoeftestellers en aanbieders niet optimaal was. Deze problemen, die nauw met elkaar samenhangen, bestaan momenteel nog steeds en kunnen ook in de toekomst blijven bestaan. Slechts op het punt van handhaving zijn sinds 2004 stappen ondernomen om deze serieus aan te pakken; feitelijk staat de handhaving echter nog in de kinderschoenen, en het is nog de vraag of het Agentschap Telecom voldoende omvang en deskundigheid zal blijken te hebben om effectief te kunnen handhaven, gezien de grote, dynamische en complexe markt. Dit is iets wat nauwlettend in de gaten gehouden zal moeten worden.
Goede handhaving zal voor een deel het probleem van weinig spontante naleving ondervangen, aangezien een deel van de aanbieders die zich nu niets aan aftapbaarheid gelegen laten liggen, er bewust van zal maken dat er wettelijke bepalingen bestaan die zij echt moeten naleven. Maar daarmee zal het probleem van gebrekkige naleving nooit geheel worden opgelost. We constateerden dat een deel van dit probleem ook veroorzaakt wordt door een niet-optimale, in sommige gevallen zelfs verstoorde, verhouding tussen behoeftestellers en aanbieders. Hoewel het onderlinge vertrouwen in de afgelopen jaren in sommige opzichten wel iets is gegroeid, door de langzaam maar gestaag toenemende kennismaking met elkaar, is het in andere opzichten eerder af- dan toegenomen, bijvoorbeeld door de gang van zaken bij de operationalekostenvergoeding (zie par. 5.2) en door het verschil van inzicht in wat de aftapbaarheid uiteindelijk oplevert. Ons algemene beeld is dat er veel wederzijds wantrouwen bestaat en dat er weinig waardering wordt geuit voor elkaars inspanningen of standpunten. Dat is verklaarbaar, door cultuurverschillen, uiteenlopende deskundigheid en een grote belangentegenstelling, maar het heeft onmiskenbaar een negatief effect op de uiteindelijke effectiviteit van de wetgeving. De aftapbaarheid en de meewerkplichten zouden beter uit de verf komen als de kloof tussen behoeftestellers en aanbieders kleiner zou zijn en er meer wederzijds begrip zou bestaan. Er zijn geen aanwijzingen dat de onderlinge verstandhouding in de komende jaren zal verbeteren, en mede door de hierna te bespreken probleemvelden dreigt de verstandhouding eerder te verslechteren dan te verbeteren.
Wij concluderen dat enerzijds de effectiviteit van beleid en wetgeving in de toekomst kan verbeteren door strakkere handhaving dan voorheen, mits AT daartoe voldoende blijkt uitgerust, maar dat anderzijds de effectiviteit negatief wordt beïnvloed door de niet-optimale verstandhouding tussen behoeftestellers en aanbieders, een negatieve invloed die in de toekomst eerder groter dan kleiner zal worden.

Probleemveld 2: aftapbaarheid bij introductie
In de vorige paragraaf constateerden wij eveneens dat een knelpunt in het huidige beleid en wetgeving is dat aftapbaarheid verondersteld wordt vanaf het moment van introductie in de markt gegarandeerd te zijn, terwijl in de praktijk de aftapbaarheid meestal enige tijd na introductie, vaak werkendeweg, wordt verzekerd. Dit probleem zal blijven bestaan – wij merkten hiervoor al op dat het onrealistisch is om aftapbaarheid op moment van introductie daadwerkelijk af te dwingen. Het zou ook onwenselijk zijn indien dit onderdeel van het beleid feitelijk zou worden afgedwongen, in het licht van bedreigingen voor innovatie en mededinging die naar ons inzicht dan zouden ontstaan die tot nu toe – doordat dit onderdeel van het beleid niet in de praktijk werd gehandhaafd – niet zijn voorgekomen. Dit onderdeel van het beleid zou dan ook moeten worden aangepast. Strakke handhaving zou wel kunnen beogen om de periode van niet- of niet-volledige aftapbaarheid zoveel mogelijk te bekorten, maar zou er niet op gericht moeten zijn om introductie van niet-aftapbare telecommunicatie geheel uit te sluiten. Daarbij merken wij op dat naarmate de onderlinge verstandhouding tussen behoeftestellers en aanbieders verbetert, ook de inspanningen van aanbieders om aftapbaarheid zo kort mogelijk na introductie te verzekeren vermoedelijk zullen toenemen. Nieuwe vormen van telecommunicatie(diensten) vragen wellicht om andere technische uitvoeringsregelgeving. Dit vraagt om discussie en/of onderzoek naar een adequate oplossing.

Probleemveld 3: simpele transponering van beleid, geen onderscheid naar techniek
Het aftapbaarheidsbeleid heeft zich geleidelijk ontwikkeld, met veelal kleine stappen, vanuit de situatie in de jaren tachtig met één telefonieaanbieder, het staatsbedrijf PTT, naar een tijd waarin het telecomlandschap radicaal is veranderd, met een enorme hoeveelheid private aanbieders van veel verschillende soorten telecommunicatie die doorlopend technisch wordt vernieuwd, in een dynamische markt. Bij die ontwikkeling zijn beleid en wetgeving feitelijk steeds simpelweg getransponeerd van de oude naar de nieuwe situatie. Toen de PTT geprivatiseerd werd, werden

afdwingbare meewerkplichten geïntroduceerd die het eerder feitelijke meewerken van de PTT consolideerden, en toen de markt werd opengesteld voor andere aanbieders, kregen deze dezelfde meewerkplichten opgelegd. En waar de enige bekende vorm van telecommunicatie – vaste telefonie – van oudsher simpel aftapbaar was en aftapbaarheid daarom wellicht als natuurlijke eigenschap van telecommunicatie werd opgevat, kregen nieuwe vormen van telecommunicatie de plicht opgelegd om diezelfde eigenschap in te bouwen, eerst voor mobiele telefonie, later voor alle andere vormen van telecommunicatie.
In de context van 1996-1998 waren deze vertaalstappen nog wel voorstelbaar gezien de toen bestaande markt en techniek, die nog relatief overzichtelijk waren; hoogstens kan men vraagtekens plaatsen bij de één-op-één transponering van de telefoniesituatie naar het Internet, dat in 1998 al behoorlijk ontwikkeld was. Het gevolg van de vertaling van de PTT-situatie naar de Telecommunicatiewet uit 1998 is echter dat nog steeds hetzelfde beleid, met dezelfde uitgangspunten, wordt gehanteerd als destijds, terwijl zowel de markt als de techniek zich radicaal hebben ontwikkeld. In het huidige complexe en dynamische telecomlandschap stuit het beleid daarom op zijn eigen grenzen. De aanname dat aftapbaarheid een natuurlijke eigenschap van telecommunicatie is, gaat al lang niet meer op, zodat doorlopend geïnvesteerd moet worden in aftapbaar maken en houden; dit nu roept in de huidige context spanningen en weerstand op vanwege de beleids- en politieke keuze uit 1996 om de investeringskosten bij de aanbieders neer te leggen, wat in de toenmalige situatie van een klein aantal grote telefonieaanbieders een redelijke keuze was, maar wat in de huidige situatie van een groot aantal, vaak kleine, aanbieders van uiteenlopende telecommunicatietechnieken niet direct een redelijke keuze hoeft te zijn. De schatting van 1% van investeringskosten bij GSM, die zonder toelichting of onderbouwing werd uitgebreid naar alle vormen van telecommunicatie als maximumschatting (zie par. 2.6.1), blijkt een te lage schatting te zijn; ook hier is de transponering van een telefoniesituatie naar Internet, maar ook naar nieuwe vormen van telefonie, te simpel gebleken. Een en ander wil niet per se zeggen dat de kostenverdeling nu anders moet worden gemaakt, maar wel dat de politieke keuze om bij elke aanbieder van telecommunicatie investeringskosten neer te leggen opnieuw moet worden gemaakt en verantwoord. En die verantwoording kan niet liggen in een historische verklaring (“zo hebben we het altijd gedaan”) maar moet gebaseerd op een argumentatie van nut en noodzaak in de huidige context van een investeringsplicht, met een reële, onderbouwde schatting van de huidige investeringskosten.
Het beleid stuit niet alleen op de grens van omvang en aantal aanbieders, maar ook op complexiteit en diversiteit van techniek. Momenteel en in de nabije toekomst ontwikkelde techniek maakt aftapbaarheid eerder moeilijker dan makkelijker (zie probleemveld 5), en dat is een reden om ook op dit vlak niet langer een automatisme te hanteren van transpositie van beleid vanuit de historische context. Het mag zo zijn dat vroeger alle telecommunicatie aftapbaar was of relatief simpel aftapbaar te maken was, maar in de huidige context gaat dat niet meer op voor alle telecommunicatie. Ook dit betekent dat, indien het uitgangspunt dat alle telecom aftapbaar moet zijn gehandhaafd wordt, dit een bewust besluit moet zijn dat zelfstandig, vanuit de huidige context, onderbouwd moet worden. En hierbij moet ook ruimte zijn voor differentiatie naar techniek: telecommunicatie is te complex en te divers om simpelweg een eenheidsbeleid te hanteren dat voor alle vormen van telecommunicatie geldt.[172] Als voorbeeld kan gelden de verplichting om identificerende gegevens bij het CIOT aan te leveren, die in de context van telefonie begrijpelijk is en goed werkt, maar die niet al te gemakkelijk naar Internet kan worden getransponeerd omdat de techniek nu eenmaal anders in elkaar zit (zie par. 4.2.2); bij dergelijke gevallen gedifferentieerd worden naar techniek, dan wel moet zelfstandig onderbouwd worden, met inachtneming van de technische verschillen, waarom een bepaalde regeling voor élke vorm van telecommunicatie gelijkelijk moet en kan worden getroffen. Het streven naar een volledig techniekonafhankelijke wetgeving is gezien de ontwikkelingen niet langer mogelijk;
Wij concluderen dat de beleidsuitgangspunten in elk geval niet per se meer adequaat zijn voor de huidige en toekomstige situatie, omdat de context waarin zij tot gelding komen radicaal is veranderd. Dit vraagt hetzij om aanpassing van het beleid, hetzij om hernieuwde bevestiging en onderbouwing van het beleid, beargumenteerd vanuit de huidige situatie.

[172] Zie voor een kritiek op de beleidsuitgangspunten “wat off-line geldt, moet ook on-line gelden” en “wetgeving moet techniekonafhankelijk zijn” de hoofdstukken van Schellekens en Koops in: TILT, *Deconstructing Prevalent Policy One-Liners. An Analysis of Starting Points for ICT Regulation*, TMC Asser Press 2005.

Probleemveld 4: openbaarheid, het aanknopingspunt van wettelijke plichten en de positie van EZ
Het beleid is geïmplementeerd in de Telecommunicatiewet, een wet die geldt voor openbare elektronischecommunicatieaanbieders. Dat is niet verwonderlijk, aangezien het beleid geënt was op de oude situatie waarbij de aftapplichten – zoals geïntroduceerd in de Wet op de telecommunicatievoorzieningen – golden voor de PTT en de nieuwe aanbieders van openbare telecommunicatie (zie probleemveld 3), zodat bij de wettelijke verankering werd aangeknoopt bij de opvolger van de Wtv, de Telecommunicatiewet. Dit betekent echter dat hiermee een vreemde eend in de TW-bijt is terecht gekomen: de aftapbaarheidsbepalingen in de Telecommunicatiewet, waaronder de niet in werking getreden bepaling van 13.7 over besloten telecommunicatie, botsen met het karakter van deze wet als marktordeningswet (zie par. 3.2). Dit spanningsveld blijkt ook in het toenemende grijze gebied van netwerken en diensten waarvan niet duidelijk is of ze openbaar zijn of niet; vanuit het oogpunt van de behoefte aan aftapbaarheid wordt dit grijze gebied anders geïnterpreteerd dan vanuit het oogpunt van marktordening. Het is dan ook de vraag of het aanknopingspunt van openbaarheid wel het meest geschikte is om aftapbaarheidsplichten in het leven te roepen: voor de behoefte tot aftappen maakt het niet zo zeer uit of telecommunicatie openbaar of besloten is, maar eerder in welke mate telecommunicatie gebruikt wordt door misdadigers en staatsgevaarlijke personen. Nu er besloten netwerken of diensten zijn die dermate groot zijn dat een substantieel deel van de telecommunicatie in Nederland via deze plaatsvindt, en anderzijds er kleine netwerkjes zijn die volgens de letter van de wet openbaar zijn maar die eigenlijk fungeren als privénetwerkjes voor een kleine kring waarbij niet direct een grote aftapbehoefte bestaat, rijst de vraag of openbaarheid het criterium moet blijven voor de aftapbaarheidsverplichtingen. In het verlengde daarvan moet men zich afvragen of het aftapbaarheidsbeleid überhaupt wel thuishoort in de Telecommunicatiewet, waar het een vreemde eend in de bijt is, en of het wel zinvol is om het Ministerie van Economische Zaken, in casu DGTP, beleidsverantwoordelijkheid te geven op een terrein waar Justitie, BZK en Defensie overwegende belangen hebben.
Nu zou men kunnen denken dat de huidige constructie zinvol is omdat in elk geval EZ een bemiddelende rol kan spelen tussen aanbieders en behoeftestellers, mede vanwege de tussen dezen bestaande spanningen (zie probleemveld 1). In de praktijk komt een dergelijke rol echter niet uit de verf. Aanbieders zien veelal de overheidsinstantie DGTP als een verlengstuk of spreekbuis van de behoeftestellers, terwijl de behoeftestellers DGTP neigen te beschouwen als een instantie die opkomt voor de economische belangen van het bedrijfsleven. In deze mangelpositie blijkt DGTP nauwelijks een zinvolle rol te kunnen spelen, en problemen tussen aanbieders en behoeftestellers moeten in de praktijk bijna altijd door dezen zelf worden opgelost. Nu is wel een voordeel van de onderbrenging in de Telecommunicatiewet hiermee geen zelfstandig criterium voor inwerkingtreding van een aftapbaarheidsplicht hoeft te worden gevonden, omdat kan worden aangesloten op het natuurlijke criterium uit deze wet, te weten openbaarheid. Maar dit criterium is, zoals boven gesteld, in de aftapcontext ongelukkig, en het ligt ook niet in de rede te veronderstellen dat het vraagstuk van besloten netwerken in de toekomst kan worden opgelost binnen de kaders van de huidige wet. In het huidige en toekomstige telecomlandschap zal een significant deel van de telecommunicatie over besloten netwerken of diensten gaan; men kan dan wel art. 13.7 TW in werking laten treden, maar dan zal aftapbaarheid van de desbetreffende netwerken alleen kunnen worden afgedwongen door een AMvB én door een vergoeding van de investeringskosten door de overheid. Aangezien het om substantiële netwerken gaat (anders zou er onvoldoende tapbehoefte zijn om een aftapbaarheidsplicht te rechtvaardigen), zullen de investeringskosten hoog zijn. Het betreft hier netwerken waarvan de architectuur noch de technische realisatie zich goed lenen voor het inbouwen van tapmogelijkheden.[173] Het lijkt ons onrealistisch dat de overheid die kosten zal willen – of kunnen – dragen. Dan kan men nog het beleid aanpassen en ook private netwerken de investeringskosten laten dragen, maar dan zou de wetgever een richting inslaan die nog minder rekening houdt met de complexe telecommunicatiecontext dan het huidige beleid doet (vgl. probleemvelden 3 en 5).

[173] Veelal gaat het hier om grote, private netwerken op basis van Ethernet- en Internettechniek. Het schakelen van verkeer vindt daarbij zo lokaal mogelijk plaats. Voor aftapbaarheid moeten ofwel tot op de kleinste locaties (*switches* in ieder kast en op iedere verdieping) nieuwe faciliteiten worden aangebracht, die vaak in het geheel niet geboden worden door de desbetreffende fabrikant, of al het verkeer moet meer central worden geschakeld, wat vraagt om een enorme uitbreiding van de transmissiefaciliteiten in het netwerk, omdat nu eenmaal zo'n 90% van het verkeer zeer lokaal van karakter is en de huidige transmissielijnen dus maar op 10% van het totale verkeer gedimensioneerd zijn.

Wij concluderen op basis van dit alles dat het criterium van openbaarheid aan heroverweging toe is, dat het vraagstuk van besloten netwerken de effectiviteit van aftapbaarheid in de toekomst meer dan in het verleden onder druk zet, en dat de onderbrenging van de aftapbaarheidsregeling in de Telecommunicatiewet niet vanzelfsprekend is.

Probleemveld 5: afnemende effectiviteit en efficiëntie door diverse technische en marktontwikkelingen

De effectiviteit van de aftapbaarheidswetgeving is tot nu toe behoorlijk groot geweest, in die zin dat het overgrote deel van de telecommunicatie wel ergens aftapbaar is (zie 8.1). Het zal moeilijk zijn – of veel investeringen vergen – om in de toekomst eenzelfde mate van aftapbaarheid te bereiken. Veel ontwikkelingen in techniek en markt zullen ervoor zorgen dat het minder makkelijk wordt telecommunicatie te tappen of afgetapte signalen te kunnen interpreteren. In welke mate de aftapbaarheid hierdoor afneemt is moeilijk te voorspellen, maar dát de aftapbaarheid minder wordt lijkt ons zeker. Hiervoor zijn vele ontwikkelingen verantwoordelijk (zie uitgebreid hfd. 7): onder andere Voice over IP (VoIP), *peer-to-peer*-toepassingen, *home-grown networking*, *seamless roaming*, een explosie van protocollen, *mesh networks*, en toenemende ingebouwde encryptie. Dit zorgt er globaal voor dat enerzijds verkeersstromen minder goed bij bepaalbare of aanspreekbare aanbieders zijn op te vragen of überhaupt niet meer bij dienstaanbieders langskomen, en anderzijds dat het tappen op netwerkniveau theoretisch wel mogelijk is maar minder individualiseerbare of interpreteerbare signalen oplevert.

Voor sommige van deze problemen zal een technische oplossing gevonden kunnen worden, maar niet voor allemaal. Met name problemen die ontstaan doordat verkeer buiten aanspreekbare aanbieders omgaat, zijn niet technisch op te lossen, behalve door de verantwoordelijken te dwingen om de toepassing wel via aanspreekbare aanbieders te laten routeren; dit zal deels extra handhaving en meer internationale afstemming en standaardisatie vergen, bijvoorbeeld omdat het aanbod vanuit het buitenland toeneemt, maar deels ook een uitbreiding van de reikwijdte van de wettelijke verplichting tot partijen die geen openbare telecommunicatie aanbieden. Bovendien levert dit aanzienlijke kosten op, niet alleen financieel, maar vooral ook in functionaliteit en efficiëntie van de dienst. Dan ontstaan serieuze bedreigingen voor innovatie en mededinging.

Nu valt dit eerste probleem nog enigszins op te vangen door meer op netwerkniveau te tappen, maar dat gaat wel ten koste van de privacy van niet-verdachte burgers wiens communicatie meeonderschept wordt. Bovendien komt hier de tweede ontwikkeling om de hoek kijken. Er valt volgens ons sowieso moeilijk aan te ontkomen om in de toekomst meer dan nu op netwerkniveau te tappen, wil men eenzelfde niveau van aftapbaarheid bereiken. Diensten zullen immers minder dan momenteel aanspreekbaar zijn, en ook zijn de juiste – dynamische – identiteiten van af te luisteren personen minder snel te achterhalen. De tijd dat slechts één vast IP-adres van een gebruiker voldoende was om een redelijk volledig beeld van de telecommunicatieactiviteiten te hebben, ligt grotendeels achter ons. Het gevolg is dat er veel meer netwerksignalen in bulk binnenkomen bij de behoeftestellers, waaruit dan de benodigde signalen gedestilleerd en geïnterpreteerd moeten worden. Dit zal voor een deel goed kunnen, zeker omdat meer en meer intelligente systemen worden ontwikkeld voor analyse van grote hoeveelheden complexe data. Een ander deel zal echter niet te achterhalen zijn door het toenemende gebruik van standaard ingebouwde encryptie (bijvoorbeeld in IPv6).

Bovendien, en belangrijker nog, is het feit dat de overheid momenteel nauwelijks is toegerust om met bulknetwerkverkeer om te gaan. Het zal niet alleen veel investeringen bij de behoeftestellers vergen in techniek en deskundigheid om dit te kunnen, maar ook een cultuuromslag. De behoeftestellers zijn immers gewend, op basis van de situatie uit het verleden en de daarop gebaseerde wetgeving, om communicatie binnen te krijgen in hapklare vorm. Wanneer de nu voorzienbare technische ontwikkelingen zich doorzetten, zal het tappen op dienstniveau geleidelijk meer gaten gaan vertonen, en zullen de behoeftestellers eraan moeten wennen dat zij meer aftapsignalen binnenkrijgen die minder direct bruikbaar zijn. Wil de effectiviteit van aftapbaarheid bij die ontwikkeling nog in de buurt blijven van het huidige niveau, dan zal flink geïnvesteerd moeten worden in techniek, kennis en attitude bij de behoeftestellers. Daarbij moet wel worden aangetekend dat het tappen op netwerkniveau, waarbij bulktelecommunicatie bij behoeftestellers binnenkomt, privacy- en controlevragen oproept die bij tappen op dienstniveau minder een rol spelen omdat er een derde partij, de aanbieder, bij betrokken is die de selectie doet. Wanneer die ingebouwde beperking vervalt, moet ook nagedacht worden over andere

vormen van *checks and balances* die voorkomen dat kennis wordt genomen van communicatie van niet-verdachte burgers die meeonderschept is.
In het verlengde van de dreigende afname in effectiviteit van de aftapbaarheidswetgeving, kan ook nog iets worden gezegd over de efficiëntie ervan. Hoewel deze in absolute zin nauwelijks te bepalen is, kan wel worden vastgesteld dat de hierboven geschetste ontwikkelingen (zie nader hfd. 7) de kosten om aftapbaarheid te verzekeren zeker niet kleiner zullen maken dan in het verleden, maar vermoedelijk zullen doen toenemen, terwijl de baten (hoe men die ook precies definieert) vanwege de afname in effectiviteit niet zullen stijgen maar eerder zullen afnemen. Met andere woorden, het is aannemelijk dat de doelmatigheid van de aftapbaarheidswetgeving in de toekomst geleidelijk zal afnemen.
Wij concluderen bij dit probleemveld dat er veel ontwikkelingen in de telecommunicatietechniek en -markt zijn die de effectiviteit van de wetgeving doen afnemen doordat er meer gaten zullen vallen in de aftapbaarheid. Deze gaten zullen voor een deel op te vangen zijn door meer op netwerkniveau te tappen en binnenkomende bulksignalen vervolgens te analyseren en interpreteren, maar dit vergt veel investeringen bij de overheid, en ook met die investeringen zal de aftapbaarheid niet het niveau halen dat nu is bereikt, maar lager liggen. En wil men een niveau van aftapbaarheid garanderen dat onvermijdelijk lager zal liggen dan het huidige maar dat nog wel voldoende ruimte biedt voor de behoeftestellers, dan zullen waarschijnlijk meer investeringen nodig zijn – zowel bij aanbieders als bij de overheid – dan voorheen; de doelmatigheid van het beleid neemt dus af.

Op basis van bovenstaande vijf probleemvelden, is de conclusie gerechtvaardigd dat bij voortzetting van de huidige beleidsuitgangspunten en de huidige wetgeving in de toekomst steeds meer knelpunten zullen ontstaan, waardoor steeds minder tegen aanvaardbare kosten een voor de behoeftestellers adequaat niveau van aftapbaarheid kan worden gegarandeerd. Op de korte termijn valt door inspanningen om serieus te handhaven en om de verstandhouding tussen behoeftestellers en aanbieders te verbeteren nog wel een behoorlijk adequaat niveau van aftapbaarheid te garanderen, enigszins vergelijkbaar met het huidige niveau. Maar telecommunicatieontwikkelingen zullen ertoe leiden dat er steeds meer gaten vallen in de aftapbaarheid die niet te dichten zijn met de huidige beleidsuitgangspunten en de huidige wetgeving. Daarom zullen keuzes gemaakt moeten worden in beleid en wetgeving, wil men het instrument aftappen ten minste in redelijke mate kunnen behouden.

9. Oplossingsrichtingen en scenario's

Onderzoeksvraag 3: Indien de beleidsuitgangspunten of de huidige wet- en regelgeving onvoldoende zijn toegesneden op de gesignaleerde telecommunicatieontwikkelingen, welke oplossingen zijn dan denkbaar die beter invulling zouden kunnen geven aan de behoeften tot aftappen van de behoeftestellers, met inachtneming van de belangen van aanbieders?
In het vorige hoofdstuk hebben wij vijf probleemvelden gesignaleerd die impliceren dat de huidige uitgangspunten en wetgeving onvoldoende zijn toegesneden op ontwikkelingen in telecommunicatie. In dit hoofdstuk geven wij een indicatie van mogelijke oplossingsrichtingen voor deze problemen, uitmondend in drie scenario's van aftapbaarheidswetgeving. Deze oplossingsrichtingen zijn indicatief en niet uitputtend, maar bedoeld als hulpmiddel voor de wetgever om een idee te krijgen van mogelijke oplossingen.

9.1. Oplossingsrichtingen

Probleemveld 1: handhaving, spontane naleving en de onderlinge verstandhouding tussen behoeftestellers en aanbieders
a) *Investeren in handhaving*: de door Agentschap Telecom ingeslagen weg van effectieve handhaving moeten worden voortgezet en uitgebouwd – handhaving is het essentiële sluitstuk van de aftapbaarheidswetgeving. De overheid dient nauwlettend in de gaten te houden of AT voldoende is toegerust, in omvang en deskundigheid, om effectieve handhaving in het huidige omvangrijke en complexe telecomlandschap uit te oefenen. Zodra blijkt dat het agentschap onvoldoende middelen heeft, dient hierin geïnvesteerd te worden.

b) *Verbeteren van de verstandhouding tussen aanbieders en behoeftestellers*: dit is een van de belangrijkste aandachtspunten, omdat de verstandhouding tussen aanbieders en behoeftestellers te wensen overlaat, terwijl een goede verstandhouding een belangrijke basisvoorwaarde is om aftapbaarheid, zowel technisch als qua medewerking met taplasten, tot stand te brengen. Nu zal er altijd een spanningsveld bestaan tussen aanbieders en behoeftestellers vanwege de grote belangentegenstelling die nu eenmaal bestaat bij aftapbaarheid, maar dit spanningsveld staat momenteel meer op scherp dan nodig is. Het zou de onderlinge verstandhouding ten goede komen als beide partijen meer moeite zouden doen te luisteren naar elkaars standpunten en zich daarin proberen in te leven, en daarbij niet te snel een beroep te doen op eigen argumenten en referentiekaders die niet door de andere partij worden gedeeld. Naar onze indruk gaan behoeftestellers er soms te makkelijk van uit dat aanbieders van alles moeten doen omdat het nu eenmaal in de wet staat; zij zouden meer overtuigingskracht hebben wanneer zij ook inhoudelijke argumenten zouden geven waarom het maatschappelijk belang gediend is door een concrete actie die van de aanbieder wordt geëist. Omgekeerd hanteren sommige aanbieders te makkelijk commerciële of te algemene privacyargumenten die bij behoeftestellers alleen maar skepsis of argwaan oproepen; aanbieders zouden meer begrip krijgen van behoeftestellers als zij op hun beurt, in hun communicatie maar ook in daadwerkelijke medewerking, een wat meer afgewogen houding of argumentatie zouden innemen.
Naast inspanningen om de communicatie te verbeteren, kunnen ook investeringen in kennis en kunde helpen om de verstandhouding te verbeteren. Het komt nu te vaak voor dat bij concrete taplasten en gegevensvorderingen misverstanden en spanningen ontstaan door gebrekkige technische kennis bij justitie, vooral op het gebied van nieuwe techniek, of door gebrekkige juridische kennis bij de aanbieders.
Tot slot zou ook meer openheid kunnen helpen om de wederzijdse stekeligheid te verminderen. Aanbieders neigen soms vaag te doen over technische vernieuwingen die zij plegen uit angst dat bedrijfsgevoelige informatie uitlekt, maar voor geheimzinnigheid lijkt ons in het overleg met de beperkte kring van behoeftestellers die de aftapspecificaties van nieuwe telecommunicatie mee helpt ontwikkelen geen reden. De justitiële behoeftestellers zouden op hun beurt meer openheid kunnen geven over de inzet van het instrument aftappen, iets wat de overheid tot nu toe – in onze ogen nogal krampachtig – verborgen houdt.[174] Zeker omdat diverse aanbieders de nodige twijfels hebben over het nut van aftapbaarheid omdat zij dit afmeten aan de mate waarin er daadwerkelijk wordt getapt, en soms ook aan de mate waarin die taps succes hebben, kan de bereidwilligheid van aanbieders om mee te werken verbeteren wanneer de overheid – in algemene zin – inzage biedt in de mate waarin justitieel[175] wordt getapt op vaste telefonie, mobiele telefonie en Internet en idealiter ook in het percentage tapzaken dat leidt tot een veroordeling. De Verenigde Staten publiceren sinds jaar en dag een dergelijk overzicht, inclusief een ‘succespercentage’, van de justitiële tapzaken, zowel op statenniveau als federaal.[176]

Probleemveld 2: aftapbaarheid bij introductie
Het element “op het moment van introductie” uit het beleidsuitgangspunt van aftapbaarheid, dat impliciet in art. 13.1 TW is opgenomen, moet niet strikt worden gehandhaafd. De wetgever en toezichthouder moeten erkennen dat het onrealistisch is dat alle telecommunicatie op het moment van introductie aftapbaar zou zijn. Behoeftestellers moeten genoegen nemen met een pragmatische benadering om kort voor en vervolgens na de introductie gezamenlijk te werken aan een spoedige oplossing voor aftapbaarheid. Met de toezichthouder op de achterhand kan ervoor worden gezorgd dat dit traject, wat bij complexere netwerken en diensten toch vaak een gezamenlijke zoektocht is, niet onnodig lang duurt.
Daarbij lijkt het ons wenselijk om voor ingrijpende vernieuwingen in de telecommunicatie – men denke aan een nieuwe generatie mobiele telefonie of een andere nieuwe infrastructuur – gebruik te maken van de mogelijkheid van art. 13.8 TW om tijdelijke ontheffing mogelijk te maken, zoals in het verleden voor Internet is gebeurd. Indien de clausule ‘in bijzondere gevallen’ van art. 13.8 TW te beperkt is om dergelijke situaties te omvatten, moet deze clausule – of de interpretatie daarvan – worden aangepast. De mogelijkheid van tijdelijke ontheffing is bij uitstek geschikt om een overgangsperiode te hebben waarin aanbieders en overheid gezamenlijk kunnen werken aan

[174] Zie noot 171.
[175] Cijfers over tappen door inlichtingen- en veiligheidsdiensten hoeven hierin niet meegenomen te worden, al lijkt ons het gevaar voor de staatsveiligheid van publicatie van het jaarlijkse *aantal* ivd-taps gering.
[176] Zie noot 171.

aftapbaarheid en aan overdrachtspecificaties, zonder dat aanbieders een zwaard van Damocles hoeven te ervaren van dreigende handhaving van een wettelijke eis waaraan zij realistischerwijs echt niet kunnen voldoen. Tijdelijke ontheffing is een nuttig instrument dat rechtszekerheid biedt, en dat aanbieders een prikkel biedt om loyaal mee te werken aan werkbare oplossingen voor aftapbaarheid, in de wetenschap dat na afloop van de ontheffing de wettelijke plicht daadwerkelijk gehandhaafd zal worden.
Bovendien schept dit ruimte om op internationaal niveau, zoals binnen ETSI, gezamenlijk te werken aan gestandaardiseerde aftapoplossingen. Bij de benodigde overdrachtspecificaties speelt immers een belangrijke rol het feit dat Nederland relatief klein is. Bij gebruik van eigen, nationale specificaties kunnen de kosten snel toenemen. Om onnodige maatschappelijke kosten te voorkomen is het van belang waar mogelijk aan te sluiten bij internationale normen en ontwikkelingen op dit gebied. Hoewel de ontwikkeling van die normen niet altijd zonder obstakels verloopt, zou Nederland zich hard moeten maken voor een voortvarende normontwikkeling en afstemming tussen landen. Zo kan voorkomen worden dat bij nieuwe technieken en diensten (denk aan VoIP) ieder land eigen, dure oplossingen kiest voor het realiseren van aftapbaarheid. Bij gebrek aan formele normen is het aansluiten bij specificaties uit andere landen, of zelfs het adopteren van een breed gedragen bedrijfsstandaard, te prefereren boven een afwijkende nationale oplossing.
Het is wel een nadeel dat een tijdelijke ontheffing een signaal kan zijn dat het netwerk of de dienst niet aftapbaar is, zodat – in de vrees van behoeftestellers – misdadigers en staatsgevaarlijke personen daar massaal gebruik van gaan maken. Aan de andere kant is het voor ingewijden (waartoe in elk geval georganiseerde misdadigers en terroristen behoren) een ervaringsgegeven dat er bij nieuwe telecommunicatie de kans bestaat dat deze in het begin vaak niet – volledig – aftapbaar is. Bij echt ingrijpende vernieuwingen in de telecommunicatie is het dan ook naïef te denken dat een ontheffing misdadigers en terroristen op een idee zal brengen dat zij anders niet al lang zouden hebben. Overigens is het aan te bevelen om in dergelijke gevallen van tijdelijke ontheffing overeen te komen dat er al wel, op ad-hocbasis, in voorkomende gevallen directe taps kunnen worden gezet, dat wil zeggen dat aanbieders moeten dulden dat de behoeftestellers met eigen aftapapparatuur langskomen en deze op een geschikte plaats in het netwerk aansluiten.[177] Dit vermindert de gevolgen van het tijdelijk niet-aftapbaar zijn, en het voorkomt eventueel anticiperend gedrag bij misdadigers.

Probleemveld 3: simpele transponering van beleid, geen onderscheid naar techniek
De beleidsuitgangspunten en de Telecommunicatiewet uit 1998 zijn geënt op de oude situatie van vaste PTT-telefonie, in stapjes getransponeerd naar nieuwe vormen van telecommunicatie en nieuwe telecomaanbieders. Deze simpele omzettingsoperatie kan niet langer worden volgehouden, omdat het telecomlandschap nu wezenlijk veranderd is. Dat betekent dat de beleidsuitgangspunten en de individuele wettelijke bepalingen nu zelfstandig moeten worden herbevestigd, onderbouwd met argumenten voor de huidige situatie, dan wel moeten worden herzien.
Zoals onze analyse van de probleemvelden aangeeft, zijn de meeste beleidsuitgangspunten en wettelijke bepalingen nog steeds houdbaar in de huidige situatie, maar geven de volgende punten aanleiding tot herziening of herbevestiging:

- het aanknopingspunt van openbaarheid;
- het uitgangspunt dat álle (openbare) telecommunicatie aftapbaar moet zijn, zonder onderscheid in techniek of aanbieder;
- het uitgangspunt dat alle aanbieders de investeringskosten dragen, wat voor kleine aanbieders een relatief zware belasting oplevert;
- het uitgangspunt dat aanbieders actuele identificerende informatie beschikbaar moeten stellen, wat voor Internet een wezenlijk andere situatie oplevert dan bij telefonie.

De eerste drie punten roepen vragen op over de reikwijdte van de aftapbaarheidsplicht; een mogelijke oplossing hiervoor is om een ander criterium te kiezen voor inwerkingtreding van de aftapbaarheidsplicht, dat aanknoopt bij omvang van de telecommunicatie in plaats van bij openbaarheid. Hierop gaan we hierna nader in (probleemveld 4).
Het laatste punt moet worden aangepakt door bewust onderscheid te maken tussen telefonie en Internet. De uitbreiding van het CIOT naar Internet kan geen automatisme zijn, omdat

[177] Sommige aanbieders zullen dit als een onaanvaardbare inbreuk op de integriteit van hun netwerk zien, maar zij hebben natuurlijk altijd de keuze om niet van de ontheffingsmogelijkheid gebruik te maken en direct al de aftapvoorzieningen te realiseren.

identificerende gegevens bij Internet veel dynamischer en complexer zijn dan bij telefonie.[178] Een constructie die moet waarborgen dat behoeftestellers bij Internet weten welke namen of nummers zij moeten aftappen, moet zelfstandig worden getroffen vanuit de Internetcontext, met oog voor de aftapbehoeften, de dynamiek van de techniek, de kosten en de gevolgen voor privacy daarbij. Hetzelfde geldt overigens voor andere aftapgerelateerde constructies die worden getroffen in het kader van hoofdstuk 13 TW, zoals de mogelijke bewaarplicht voor verkeersgegevens (zie par. 2.5.6): ook daarbij moet worden gedifferentieerd tussen telefonie en Internet omdat hierbij fundamenteel verschillende situaties bestaan, waardoor eenheidsworstwetgeving onrechtvaardige gevolgen dreigt te hebben voor een deel van de techniek. Meer in het algemeen geldt daarom ook dat de Nederlandse overheid niet strikt moet vasthouden aan het uitgangspunt dat wetgeving techniekonafhankelijk moet zijn: wil men in wetgeving belangen waarborgen en een bepaalde balans treffen tussen strijdende belangen, dan is soms juist onderscheid naar techniek aangewezen om dit te bereiken.

Probleemveld 4: openbaarheid, het aanknopingspunt van wettelijke plichten en de positie van EZ
Wij concludeerden hierboven dat het criterium van openbaarheid aan heroverweging toe is, dat het vraagstuk van besloten netwerken de effectiviteit van aftapbaarheid in de toekomst meer dan in het verleden onder druk zet, en dat reflectie nodig is op de onderbrenging van de aftapbaarheidsregels in de Telecommunicatiewet en op de positie van DGTP hierbij.
In plaats aan te knopen bij openbaarheid als criterium voor het gelden van aftapbaarheidsplichten, zou gezocht moeten worden naar een ander criterium dat beter past bij het doel van de wet: zekerstellen van aftapbaarheid in het licht van de behoefte van de overheid aan aftappen. Daarvoor komt onzes inziens vooral een criterium dat aanknoopt bij omvang in aanmerking: naarmate er meer telecommunicatie plaatsvindt, neemt de behoefte aan aftappen toe, en omgekeerd.[179] Men kan omvang afmeten aan verschillende punten: de omvang van de aanbieder (aantal fte), de omvang of systeemcapaciteit van het netwerk of de dienst in fysieke zin, de omvang in aantal gebruikers (aantal abonnees en/of aantal mensen dat gebruikt maakt van het netwerk of de dienst), en de omvang in telecommunicatieverkeer (aantal 'communicatiehandelingen' en/of aantal kilobytes). De omvang van de aanbieder of van het fysieke netwerk lijkt ons niet direct een geschikt criterium, aangezien ook kleine aanbieders of netwerken veel telecomgebruikers of -verkeer kunnen hebben; de behoefte aan aftappen ontstaat juist waar veel gebruikers bestaan of veel telecommunicatie wordt uitgewisseld. Aan de andere kant ligt het in verband met de kostentoerekening ook voor de hand te kijken naar de omvang van de aanbieder in personeel en in jaaromzet; dit zal vaak samenhangen met het aantal gebruikers of de omvang van het verkeer, maar dat is niet altijd het geval. Het is dan ook niet evident hoe het criterium van omvang moet worden geoperationaliseerd, maar het verdient aanbeveling te onderzoeken hoe dit op korte termijn gerealiseerd kan worden. Dat is des te meer aangewezen, omdat het vraagstuk van besloten netwerken blijft bestaan en de huidige constructie van art. 13.7 (private netwerken zijn bij AMvB aftapbaar te maken op kosten van de overheid) daarvoor geen geschikte oplossing lijkt te bieden. Met het zoeken naar een ander criterium voor aftapbaarheidsplichten kan dan tegelijk worden nagedacht of en hoe aanbieders van substantiële besloten netwerken of diensten verplicht zouden moeten worden aftapbaarheid te garanderen. Bij dit alles speelt tot slot ook nog de kostenverdeling een rol, die nu kleine aanbieders een relatief zware lastenpost oplegt.
Wij schatten in dat het uiteindelijk doelmatiger zal zijn om een aftapbaarheidsplicht op te leggen aan partijen die telecommunicatie faciliteren met een bepaalde, nader te definiëren, minimumomvang. Onder die drempelwaarde hoeft men dan niet op eigen kosten aftapbaarheid in te bouwen, maar moet men wel dulden dat de behoeftestellers zelf langskomen om eigen tapapparatuur op het netwerk aan te sluiten. Een dergelijke constructie betekent dat kleine

[178] De periode waarop een Internet-identiteit als stabiel kan worden gezien is soms zo kort, tot op enkele seconden, dat er een onacceptabel grote onzekerheid ontstaat of deze identiteit op het moment van aftappen wel echt toebehoort aan de beoogde persoon.
[179] Saillant is dat de wetgever eigenlijk ook omvang lijkt te hebben bedoeld als het criterium voor aftapbaarheid. Bij de behandeling van de Telecommunicatiewet is immers opgemerkt dat er enerzijds openbare netwerken of diensten zijn 'waarvan de noodzaak om die te kunnen aftappen geen noemenswaardige betekenis heeft', en anderzijds dat soms bij niet-openbare netwerken of diensten 'de kring van gebruikers zodanig ruim is dat aftapbaarhied [sic] toch noodzzakelijk [sic] is in verband met genoemde belangen' van opsporing en staatsveiligheid. *Kamerstukken II* 1997/98, 25 533, nr. 3, p. 127 resp. nr. 5,p. 133-134. Uit deze citaten blijkt dat de wetgever zich heeft gerealiseerd dat openbaarheid als criterium niet parallel loopt met de behoefte aan aftapbaarheid, en dat eerder het aanknopingspunt voor een aftapbaarheidsplicht is het feitelijk gebruik dat van een netwerk of dienst wordt gemaakt in het licht van de behoefte aan aftappen.

vormen van telecommunicatie, waar relatief weinig aftapbehoefte bestaat, niet tegen relatief hoge maatschappelijke kosten aftapbaar hoeven te worden gemaakt, zonder dat de mogelijkheid om af te tappen geheel verdwijnt – de overheid kan immers zelf investeren in een aftapfaciliteit à la het NBIP-aftapkastje.
In het verlengde van het zoeken naar een nieuw criterium voor aftapbaarheid, kan ook worden nagedacht over de wettelijke inbedding van de aftapbaarheidsplichten. De invoeging in de Telecommunicatiewet botst met het karakter van die wet als marktordeningswet voor openbare elektronische communicatie. Zeker wanneer afgestapt wordt van het criterium van openbaarheid, moet overwogen worden om aftapbaarheid in een afzonderlijke wet te regelen. Maar ook bij handhaving van openbaarheid als aanknopingspunt voor aftapbaarheidsplichten, heeft een zelfstandige wet voordelen boven de huidige situatie, namelijk erkenning van de eigenheid van de problematiek en de andersoortige belangen die hierbij een rol spelen. Daarmee wordt ook verzekerd dat er een zelfstandig parlementair debat wordt gevoerd met oog voor deze belangen, in plaats van een debat in de marge van de veel omvangrijkere en andersoortige problematiek van de Telecommunicatiewet. Het biedt ook de mogelijkheid om de wet onder beleidsverantwoordelijk te brengen van de meest betrokken ministeries, Justitie, BZK en Defensie; de inbedding bij het ministerie van EZ heeft geen duidelijke meerwaarde in de praktijk.

Probleemveld 5: afnemende effectiviteit en efficiëntie door diverse technische en marktontwikkelingen
Op termijn zal de effectiviteit van aftapbaarheidsplichten afnemen, naarmate er meer verkeer plaatsvindt dat niet via aanspreekbare dienstaanbieders te verkrijgen valt en naarmate netwerkverkeer moeilijker te herleiden is tot individuele, af te tappen telecommunicatie die interpreteerbaar is. Beter dan nu zal het niet worden, maar vermoedelijk wel slechter. Dat betekent dat voor de langere termijn reflectie nodig is over de vraag hoe de overheid moet omgaan met verminderde betekenisvolle aftapbaarheid. Het is een open vraag of er oplossingen bestaan die een niveau van aftapbaarheid kunnen garanderen dat tenminste nog in de buurt komt bij het huidige niveau; als die er zijn, zullen zij volgens ons meer investeringen vergen dan de toch al substantiële investeringen die in het verleden gepleegd zijn, en in elk geval zal de overheid zelf veel meer moeten investeren in techniek en deskundigheid om adequaat om te kunnen gaan met netwerktaps. Tegelijkertijd moet ook rekening worden gehouden met een langetermijnscenario waarin de mogelijkheid van betekenisvol aftappen significant afneemt en waarin in elk geval een verschuiving plaatsvindt van het onderscheppen van inhoud van communicatie naar het verkrijgen van verkeersgegevens. De overheid kan het zich in dat licht niet veroorloven aftappen als wondermiddel te (blijven) beschouwen voor de opsporing en voor de bescherming van de staatsveiligheid.
Wij adviseren om in de komende vijf jaar na te gaan of deze verwachte tendens van afname in betekenisvol tappen zich inderdaad voordoet Daarbij verdient het overweging om de komende jaren centraal en onafhankelijk – bijvoorbeeld door het Agentschap Telecom – te laten registreren hoeveel taplasten worden gegeven op netwerk- en op dienstenniveau, hoeveel gewenste taplasten niet worden gegeven omdat de behoeftestellers van niet-aftapbaarheid uitgaan, hoeveel van de gegeven lasten worden uitgevoerd en hoeveel lasten stuiten op technische problemen, zowel in het onderscheppen van het signaal als in het interpreteren van het signaal[180].[181] Ondertussen moet de overheid onderzoeken welke mogelijkheden er zijn om deze verwachte tendens tegen te gaan of om te buigen en hoeveel dat dan kost, in termen van financiële investeringen bij aanbieders en overheid, maar ook in termen van gevolgen voor innovatie, mededinging en privacy. Als blijkt dat de tendens zich daadwerkelijk voordoet en niet, of alleen tegen buitensporige kosten, tegengegaan kan worden, dan zal de overheid zich op dat moment kritisch moeten bezinnen op de waarde van het instrument aftappen ten opzichte van andere opsporingsmethoden.

[180] In de VS wordt bij de tapcijfers (zie noot 171) ook geregistreerd in hoeveel gevallen encryptie werd aangetroffen en hoe vaak dat tot problemen leidde. In 2004 kwamen twee gevallen voor van encryptiegebruik bij taps, waarbij de opsporingsdiensten desondanks de klare tekst van de communicatie wisten te achterhalen, aldus <http://www.uscourts.gov/wiretap04/2004WireTap.pdf>, p. 5.
[181] Wij realiseren ons dat een eerder initiatief van de behoeftestellers om problemen bij de uitvoering van taps te registreren is stopgezet, maar wij achten een onafhankelijke registratie van dermate groot belang voor een zorgvuldige evaluatie van de aftapbaarheidswetgeving, dat de overheid hiervoor aparte middelen beschikbaar zou moeten stellen.

9.2. Scenario's

Een beschouwing van de hierboven gegeven mogelijke oplossingsrichtingen leert dat deze kunnen worden samengevat in drie scenario's die het aftapbaarheidsbeleid elk verschillend invullen.

A. Het huidige beleid en de huidige wetgeving worden voortgezet: alle openbare telecommunicatienetwerken en -diensten moeten aftapbaar zijn voor de marktintroductie.
B. Aanpassingen in de afbakening: in plaats van openbaarheid is de – nader te operationaliseren – omvang van een telecommunicatienetwerk of -dienst maatgevend voor de gelding van een aftapbaarheidsplicht. Indien de telecommunicatie een minimumomvang heeft, moet de aanbieder of beheerder hiervan aftapbaarheid inbouwen op eigen kosten en meewerken met taplasten van behoeftestellers. Onder de drempelwaarde is de aanbieder of beheerder niet verplicht te investeren in aftapbaarheid (al mag hij dat vrijwillig doen), maar is hij wel verplicht te dulden dat behoeftestellers zelf zijn dienst of netwerk komen aftappen.
C. Concentratie op netwerktaps: in plaats van diensten af te tappen, richt de overheid zich op netwerktaps waarbij op netwerkniveau bulkverkeer wordt onderschept waarin vervolgens – door de overheid zelf, of door een derde partij op kosten van de overheid – de te onderscheppen signalen worden uitgefilterd en geïnterpreteerd. Een netwerktap maakt een ernstige inbreuk op de privacy, omdat veel meer verkeer wordt onderschept dan de beoogde af te tappen communicatie, zodat extra maatregelen nodig zijn om de toename van de privacyinbreuk zo beperkt mogelijk te houden.

Wij voorzien substantiële problemen bij het scenario A in de mate van aftapbaarheid die op langere termijn bereikt kan worden en bij de toenemende kosten die een hoog niveau van aftapbaarheid zal vergen, niet alleen bij aanbieders, maar ook bij de overheid in de vorm van investeringen in handhaving en in eigen deskundigheid.
Scenario C is in bepaalde opzichten aantrekkelijk, omdat het de verantwoordelijkheid voor aftapbaarheid bij een beperkt aantal partijen legt en de dienstenmarkt ongemoeid laat. In andere opzichten is het bepaald minder gunstig: het vergt grote investeringen bij de overheid om effectief om te kunnen gaan met netwerktaps. De ernstige inbreuk op de privacy bij netwerktaps vraagt om extra *checks and balances* die het wegvallen van de aanbieder bij het selecteren van af te tappen informatie, waardoor een natuurlijke rem is ingebouwd op ongebreidelde taps, kunnen compenseren, en dit scenario kan alleen worden gevolgd als dergelijke aanvullende *checks and balances* effectief en haalbaar zijn. Misschien is dit scenario op de lange termijn het enige mogelijke, als de vele technische en marktontwikkelingen zich doorzetten die de effectiviteit van aftapbaarheid naar verwachting doen afnemen, maar voor dit moment lijkt het ons twee bruggen te ver.
Scenario B heeft daarom onze voorkeur. Daarom bevelen wij aan scenario B uit te werken, mogelijk uitmondend in een wetsvoorstel tot herziening van hoofdstuk 13 Telecommunicatiewet, of wellicht als zelfstandige wet. Met scenario B kan naar onze inschatting een behoorlijke mate van aftapbaarheid bereikt worden waardoor het instrument aftappen de komende tien tot vijftien jaar, zij het wellicht in afnemende mate, zinvol kan worden ingezet. Omdat ook in dit scenario substantiële kosten gemaakt moeten worden door zowel aanbieders als overheid, terwijl het algehele niveau van aftapbaarheid zeker niet zal toenemen, moet ondertussen ook scenario C worden afgetast; wellicht is dat op de lange termijn zelfs het enige realistische, maar onaantrekkelijke, scenario voor doeltreffende en doelmatige aftapbaarheid.

9.3. Samenvatting van oplossingsrichtingen

In onderstaande tabel geven wij een samenvatting van mogelijke oplossingsrichtingen voor de gesignaleerde problemen. Wij formuleren de oplossingen in de vorm van aanbevelingen.

probleemveld	aanbevelingen
1: handhaving, spontane naleving en de onderlinge verstandhouding tussen behoeftestellers en aanbieders	• De handhaving door Agentschap Telecom moet worden voortgezet en uitgebouwd, zeker waar achterstanden zijn ontstaan ten aanzien van het aftapbaar maken van systemen; de overheid moet zo nodig extra investeren in handhaving; • de verstandhouding tussen aanbieders en behoeftestellers

	moet worden verbeterd door inspanningen aan beide kanten om beter te communiceren, door investeringen in kennis en kunde op de werkvloer (niet alleen maar wel met name bij de behoeftestellers), en door meer openheid (bij aanbieders over technische ontwikkelingen, en bij de overheid over gebruik en nut van het instrument aftappen).
2: aftapbaarheid bij introductie	• De eis dat aftapbaarheid *op het moment van introductie* is verzekerd, moet niet strikt worden gehandhaafd; • bij ingrijpende vernieuwingen in de telecommunicatie moet het instrument ontheffing (art. 13.8 TW) worden gebruikt om een overgangssituatie te scheppen waarin gezamenlijk, bij voorkeur in Europees verband, aan aftapbaarheid kan worden gewerkt; zo nodig moet daartoe (de interpretatie van) de clausule 'in bijzondere gevallen' van art. 13.8 worden aangepast; • bij ontheffingverlening kan worden gestipuleerd dat de aanbieder moet dulden dat de behoeftestellers zelf op zijn netwerk of dienst komen tappen; • Nederland zou zich kunnen inspannen voor de ontwikkeling van Europese en internationale normen en voor afstemming tussen EU-lidstaten waar het de overdrachtstechnieken betreft.
3: te simpele transponering van beleid, de wetgeving is te techniekonafhankelijk	• De wetgever moet alle beleidsuitgangspunten en individuele wettelijke bepalingen, waaronder de kostenverdeling, zelfstandig hetzij herbevestigen hetzij herzien, onderbouwd met argumenten voor de huidige situatie, en niet langer redeneren vanuit de historische situatie; • de wetgever moet bij aftapgerelateerde wetgeving, zoals het CIOT en bij een eventuele algemene bewaarplicht voor verkeersgegevens, onderscheid maken tussen telefonie en Internet omdat daar fundamenteel verschillende situaties bestaan.
4: openbaarheid, het aanknopingspunt van wettelijke plichten, relatief hoge kosten voor kleine netwerken of diensten, en de positie van EZ	• De wetgever moet overwegen het criterium van openbaarheid als aanknopingspunt voor de aftapbaarheidsplichten te vervangen door een ander criterium; • het verdient sterke overweging om, in plaats van het huidige regime, de aftapbaarheidsplichten slechts op te leggen aan partijen die telecommunicatie faciliteren met een bepaalde minimumomvang; onder de drempelwaarde hoeft men niet op eigen kosten aftapbaarheid in te bouwen, maar moet men wel dulden dat de behoeftestellers zelf langskomen om eigen tapapparatuur aan te sluiten; • het verdient overweging de aftapbaarheidsplichten uit de Telecommunicatiewet te halen en onder te brengen in een zelfstandige wet onder verantwoordelijkheid van Justitie, BZK en Defensie.

5: afnemende effectiviteit en efficiëntie door diverse technische en marktontwikkelingen	• De overheid dient de komende jaren na te gaan of de door ons verwachte tendens van afname in betekenisvol tappen zich inderdaad voordoet; • de overheid dient te onderzoeken welke mogelijkheden er zijn om deze eventuele afname tegen te gaan, en hoeveel die mogelijkheden kosten, zowel qua financiële investeringen bij aanbieders en overheid, als qua gevolgen voor innovatie, mededinging en privacy; • de overheid dient in de beleidsvorming rond opsporingsmethoden rekening te houden met de mogelijkheid van een langetermijnscenario waarin het vermogen om betekenisvol af te tappen significant afneemt, tenzij tegen buitensporige kosten; • om een te grote terugval te voorkomen in de mate van betekenisvolle aftapbaarheid zal het nodig zijn substantieel te investeren in kennis, menskracht en apparatuur bij de behoeftestellers.

Bijlage I. Beleidsvoornemens 1996

1. De internationale vereisten, zoals gevoegd bij de Resolutie van de Raad van de Europese Unie van 17 januari 1995 inzake het bevoegd aftappen, dienen als uitgangspunten voor het aftapbaar maken van telecommunicatiesystemen in Nederland.

2. Alle telecommunicatienetwerken en -diensten, welke bestemd en toegankelijk zijn voor het algemene publiek, dienen (vanaf het moment van introductie) aftapbaar te zijn.

3. Ook de aftapverantwoordelijkheden van de dienstenleverancier, naast die van de netwerkbeheerder, worden bij wet geregeld (geen ketenaansprakelijkheid).

4. Netwerkbeheerders en dienstenleveranciers dienen een adequaat, bij wet opgedragen, beveiligingsregime in te richten.

5. De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen in verband met het aftappen en de informatieverstrekking alsmede in verband met de beveiliging zijn ten laste van de netwerkbeheerders respectievelijk de dienstenleveranciers.

6. De bevoegde instanties blijven de kosten betalen die gepaard gaan met de inrichting van tapkamers, de huur van aftaplijnen en de zogenaamde direkte kosten (i.e. de personeels- en administratiekosten) per individuele tap of informatieverstrekking. De Minister van Binnenlandse Zaken blijft de kosten voor de veiligheidsonderzoeken betalen.

7. Voor reeds operationele systemen betalen de Minister van Justitie en de Minister van Binnenlandse Zaken, overeenkomstig een door hen vast te stellen verdeelsleutel, eenmalige overgangsvergoedingen ten behoeve van het aftapbaar maken daarvan. Deze overgangsvergoedingen zijn f 2,9 miljoen groot. Dit bedrag is de helft van de totale investeringskosten om de reeds operationele systemen aftapbaar te maken. Daarmee komen dus ook f 2,9 miljoen ten laste van de netwerkbeheerders.

8. De wettelijk verplichte informatievoorziening door netwerkbeheerders en dienstenleveranciers wordt door de verspreiding van die informatie complex. De problematiek zal worden onderzocht opdat binnen een half jaar ter zake voorstellen gedaan kunnen worden.

9. Onderzocht wordt of, en zo ja hoe, een wettelijke informatieplicht van netwerkbeheerders en dienstenleveranciers ten behoeve van de BVD kan worden gecreëerd. Tevens wordt de «dealer»problematiek nader onderzocht. Dienaangaande zullen zo snel mogelijk voorstellen worden gedaan.

Bron: Kamerstukken II 1995/96, 24 679, nr. 1, p. 14-15

Bijlage II. Hoofdstuk 13 Telecommunicatiewet (15/12/98)

Hoofdstuk 13. Bevoegd aftappen

Artikel 13.1
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.
2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

Artikel 13.2
1. Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.
2. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last tot het aftappen of opnemen van door hen verzorgde telecommunicatie.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

Artikel 13.3
Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot het beslechten van geschillen tussen aanbieders en de bevoegde autoriteiten over de voorzieningen door middel van welke de door een tap te verkrijgen telecommunicatie door aanbieders wordt doorgegeven.

Artikel 13.4
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht aan de autoriteiten de informatie te verstrekken die noodzakelijk is om die autoriteiten in staat te stellen de bij de wet in het belang van de strafvordering of in het belang van de veiligheid van de staat geregelde bevoegdheden tot het aftappen of opnemen van telecommunicatie, dan wel tot het vorderen van gegevens ter zake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten, plaatsvindt, te kunnen uitoefenen. Deze verplichting omvat in ieder geval het desgevraagd aan de autoriteiten meedelen van het aan een gebruiker verleende nummer en de door hem afgenomen openbare telecommunicatiedienst, en het desgevraagd aan de autoriteiten meedelen van de bij een nummer behorende naam-, adres-, postcode- en woonplaatsgegevens.
2. Indien de in het eerste lid bedoelde informatie niet bij de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten bekend is, zijn zij verplicht de informatie te achterhalen en te verstrekken op een bij algemene maatregel van bestuur te bepalen wijze. Teneinde aan deze verplichting te kunnen voldoen, bewaren de aanbieders de daartoe benodigde, bij algemene maatregel van bestuur aan te wijzen gegevens, voor een termijn van drie maanden, nadat de gegevens voor het eerst zijn verwerkt.
3. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze van verstrekking van de informatie, bedoeld in het eerste lid, en de wijze waarop daartoe de gegevens beschikbaar worden gehouden.

Artikel 13.5
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last als bedoeld in artikel 13.2 en informatieverstrekkingen als bedoeld in artikel 13.4 te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.
2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging, bedoeld in het eerste lid.

Artikel 13.6
1. De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn of worden gemaakt teneinde te kunnen voldoen aan de artikelen 13.1, 13.4, en 13.5 komen te hunner laste.
2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hebben aanspraak op vergoeding uit 's Rijks kas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een bijzondere last als bedoeld in artikel 13.2, eerste en tweede lid, onderscheidenlijk het verstrekken van informatie als bedoeld in artikel 13.4.
3. Bij ministeriële regeling worden regels gesteld met betrekking tot de vaststelling en vergoeding van de kosten, bedoeld in het tweede lid.

Artikel 13.7 [niet in werking getreden]
1. Onze Minister kan in het belang van de veiligheid van de staat of de handhaving van de strafrechtelijke rechtsorde bij beschikking bepalen dat een of meer artikelen van dit hoofdstuk, met uitzondering van artikel 13.6, van overeenkomstige toepassing zijn op aanbieders van een niet-openbaar telecommunicatienetwerk, een niet-openbare telecommunicatiedienst of aanbieders van huurlijnen indien het netwerk, de dienst of een huurlijn feitelijk openstaat voor derden.
2. In het geval toepassing wordt gegeven aan het bepaalde in het eerste lid geldt dat de betreffende aanbieders aanspraak hebben op een vergoeding uit 's Rijks kas voor de in artikel 13.6, eerste lid, bedoelde investerings-, exploitatie- en onderhoudskosten voor technische voorzieningen die zijn of worden gemaakt tengevolge van de toepassing van het eerste lid. Artikel 13.6, tweede en derde lid, is van overeenkomstige toepassing.

Artikel 13.8
Van de verplichtingen die voortvloeien uit dit hoofdstuk kan Onze Minister in overeenstemming met Onze Minister van Binnenlandse Zaken en Onze Minister van Justitie in bijzondere gevallen ontheffing verlenen. Een ontheffing kan onder beperkingen worden verleend. Aan een ontheffing kunnen voorschriften worden verbonden.

Bijlage III. Hoofdstuk 13 Telecommunicatiewet (01/07/05)

Hoofdstuk 13. Bevoegd aftappen

Artikel 13.1
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.
2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

Artikel 13.2
1. Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.
2. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van door hen verzorgde telecommunicatie.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

Artikel 13.2a
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126n of artikel 126u van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens over een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst en het telecommunicatieverkeer met betrekking tot die gebruiker.
2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan de vordering of het verzoek voldoen en de wijze waarop de gegevens, bedoeld in het eerste lid, beschikbaar worden gehouden.

Artikel 13.3
Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot het beslechten van geschillen tussen aanbieders en de bevoegde autoriteiten over de voorzieningen door middel van welke de door een tap te verkrijgen telecommunicatie door aanbieders wordt doorgegeven.

Artikel 13.4
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, eerste lid, of 126ua, eerste lid, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst.
2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, tweede lid, of 126ua, tweede lid, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het op bij algemene maatregel van bestuur te bepalen wijze achterhalen en verstrekken van de gegevens, bedoeld in het eerste lid. Teneinde aan deze verplichting te kunnen voldoen bewaren de aanbieders bij algemene maatregel van bestuur aan te wijzen gegevens voor een periode van drie maanden, vanaf het tijdstip waarop deze gegevens voor de eerste maal zijn verwerkt.
3. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan een vordering of een verzoek, bedoeld in het eerste en tweede lid, voldoen en de wijze waarop de gegevens, bedoeld in het eerste lid, beschikbaar worden gehouden.

Artikel 13.5
1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2 dan wel een vordering of een verzoek als bedoeld in artikel 13.2a of artikel 13.4, eerste of tweede lid te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.
2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging, bedoeld in het eerste lid.

Artikel 13.6
1. De investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn of worden gemaakt teneinde te kunnen voldoen aan de artikelen 13.1, 13.4, en 13.5 komen te hunnen laste.
2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hebben aanspraak op vergoeding uit 's Rijks kas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, dan wel een vordering of een verzoek als bedoeld in artikel 13.2a of artikel 13.4, eerste of tweede lid.
3. Bij ministeriële regeling worden regels gesteld met betrekking tot de vaststelling en vergoeding van de kosten, bedoeld in het tweede lid.

Artikel 13.7 [niet in werking getreden]
1. Onze Minister kan in het belang van de veiligheid van de staat of de handhaving van de strafrechtelijke rechtsorde bij beschikking bepalen dat een of meer artikelen van dit hoofdstuk, met uitzondering van artikel 13.6, van overeenkomstige toepassing zijn op aanbieders van een niet-openbaar telecommunicatienetwerk, een niet-openbare telecommunicatiedienst of aanbieders van huurlijnen indien het netwerk, de dienst of een huurlijn feitelijk openstaat voor derden.
2. In het geval toepassing wordt gegeven aan het bepaalde in het eerste lid geldt dat de betreffende aanbieders aanspraak hebben op een vergoeding uit 's Rijks kas voor de in artikel 13.6, eerste lid, bedoelde investerings-, exploitatie- en onderhoudskosten voor technische voorzieningen die zijn of worden gemaakt tengevolge van de toepassing van het eerste lid. Artikel 13.6, tweede en derde lid, is van overeenkomstige toepassing.

Artikel 13.8
Van de verplichtingen die voortvloeien uit dit hoofdstuk kan Onze Minister in overeenstemming met Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties, Onze Minister van Defensie en Onze Minister van Justitie in bijzondere gevallen ontheffing verlenen. Een ontheffing kan onder beperkingen worden verleend. Aan een ontheffing kunnen voorschriften worden verbonden.

Bijlage IV. Geïnterviewde instanties en personen

behoeftestellers
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Korps Landelijke Politiediensten (KLPD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Ministerie van Justitie, Platform Interceptie, Decryptie en Signaalanalyse (PIDS)
Openbaar Ministerie

aanbieders
KPN
MCI
NLIP
Orange
Tele2
Unet
Versatel
Vodafone
XS4ALL

overig
Agentschap Telecom
Bits of Freedom
Centraal informatiepunt onderzoek telecommunicatie (CIOT)
College Bescherming Persoonsgegevens (CBP)
Directoraat-Generaal Telecom en Post (DGTP)
Fred Eisner, zelfstandige
Cyrille Fijnaut, Universiteit van Tilburg
Nederlands Forensisch Instituut (NFI)
OPTA
Jan Smits, Technische Universiteit Eindhoven
TNO

Bijlage V. Samenstelling van de begeleidingscommissie

J.C.Th. van der Doef, voorzitter Overlegorgaan Post en Telecommunicatie (voorzitter)

prof.dr. N.A.N.M. van Eijk, Universiteit van Amsterdam

prof.dr. M.J. van den Hoven, Technische Universiteit Delft

prof.mr. H.W.K. Kaspersen, Vrije Universiteit te Amsterdam

M.A. Westerhof, ministerie van Economische Zaken (secretaris)

Bijlage VI. Onderzoekers

Dr. Bert-Jaap Koops is universitair hoofddocent bij het TILT – Centrum voor Recht, Technologie en Samenleving van de Universiteit van Tilburg. Hij doet onderzoek naar strafrecht en technologie, in het bijzonder opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie, informatiebeveiliging en DNA, en naar onderwerpen als identificatie, elektronische handtekeningen, digitale grondrechten en algemene uitgangspunten van ICT-recht. Vanaf 2004 leidt hij een onderzoeksprogramma over recht, techniek en schuivende machtsverhoudingen. Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografieregulering. Koops promoveerde in januari 1999 op het proefschrift *The Crypto Controversy*. In 2002 publiceerde hij *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002*, en onlangs redigeerde hij een monografie *Strafrecht en ICT*.

Dr.ir.ing. Rudi Bekkers is senior onderzoeker en adviseur bij Dialogic innovatie & interactie en specialist in mobiele en vaste telecommunicatie, telecommunicatierecht, normalisatie en intellectueel eigendomsrecht. Hij is tevens verbonden aan de Technische Universiteit Eindhoven (Eindhoven Centre for Innovation Studies – ECIS). Naast telecommunicatie is hij actief binnen verschillende andere technologische domeinen. Binnen Dialogic is hij onder meer nauw betrokken bij projecten met betrekking tot de aanleg van breedbandige toegangsnetwerken en projecten over intellectueel eigendomsrecht, o.a. in OECD-verband. Ook is hij actief in projecten op het gebied van telecommunicatieregelgeving, normalisatie en technologische trajecten. Rudi Bekkers promoveerde in 2000 aan de Technische Universiteit Eindhoven op de ontwikkeling van GSM en andere Europese mobiele normen, schreef meer dan vijf handboeken over GSM en UMTS (ook internationaal) en heeft meer dan vijf jaar opleidingen over GSM, UMTS en verwante technologieën verzorgd voor medewerkers van KPN Mobile.

Dr. Frank Bongers studeerde beleids- en organisatiewetenschappen aan de Universiteit van Tilburg (UvT). In 2000 promoveerde hij aan de UvT op een beleidssociologische studie naar *group support systems* (lokale computernetwerken) als een innovatie in publieke besluitvorming. Hij is gespecialiseerd in de inzet van participatieve en interactieve methoden ter ondersteuning van beleidsprocessen en beleidsonderzoek, bijvoorbeeld burgerconsultaties en -panels, gaming/simulation, Internetdebatten, interactieve evaluaties en (scenario)workshops. Zijn werkterrein bestrijkt overheid, technologie en samenleving, in het bijzonder e-government. Hij verricht ook onderzoek voor overheidsbeleid gericht op technologie en innovatie, naar bijvoorbeeld internationale kennisstromen, innovatiegames, kennisuitwisseling en stimuleringsbeleid voor wetenschappelijk onderzoek. Een ander onderzoeksdomein betreft breedband en de gebruiker en computers en Internet in het onderwijs.

Ir. Marieke Fijnvandraat werkt sinds augustus 2003 als onderzoeker/adviseur bij Dialogic, met als aandachtsgebieden (breedband-)Internet en telecommunicatie. Zij is onder meer betrokken bij projecten over de aanleg van breedbandige toegangsnetwerken en over telecommunicatieregelgeving. Haar specialismen liggen bij infrastructuurconcurrentie en regulering, alternatieve breedband *local loop*-technieken en algemene telecommunicatie. Marieke Fijnvandraat studeerde in juni 2003 af in Techniek, Bestuur en Management aan de TU Delft met als afstudeeronderwerp ‘Breedband en de local loop: Innovatie, acceleratie, domesticatie’. Tijdens haar studie participeerde zij aan de TU Delft in een project over techniekonafhankelijke regulering van telecommunicatiemarkten in Europa (in samenwerking met het IvIR in Amsterdam) en in onderzoek naar Internet en interconnectie in de VS, het VK en Nederland. Vanaf 1 mei 2004 is Marieke Fijnvandraat deeltijd promovenda aan de TU Delft op een onderzoek naar technische, economische en bestuurlijke aspecten rondom ontwikkelingspaden in breedband.